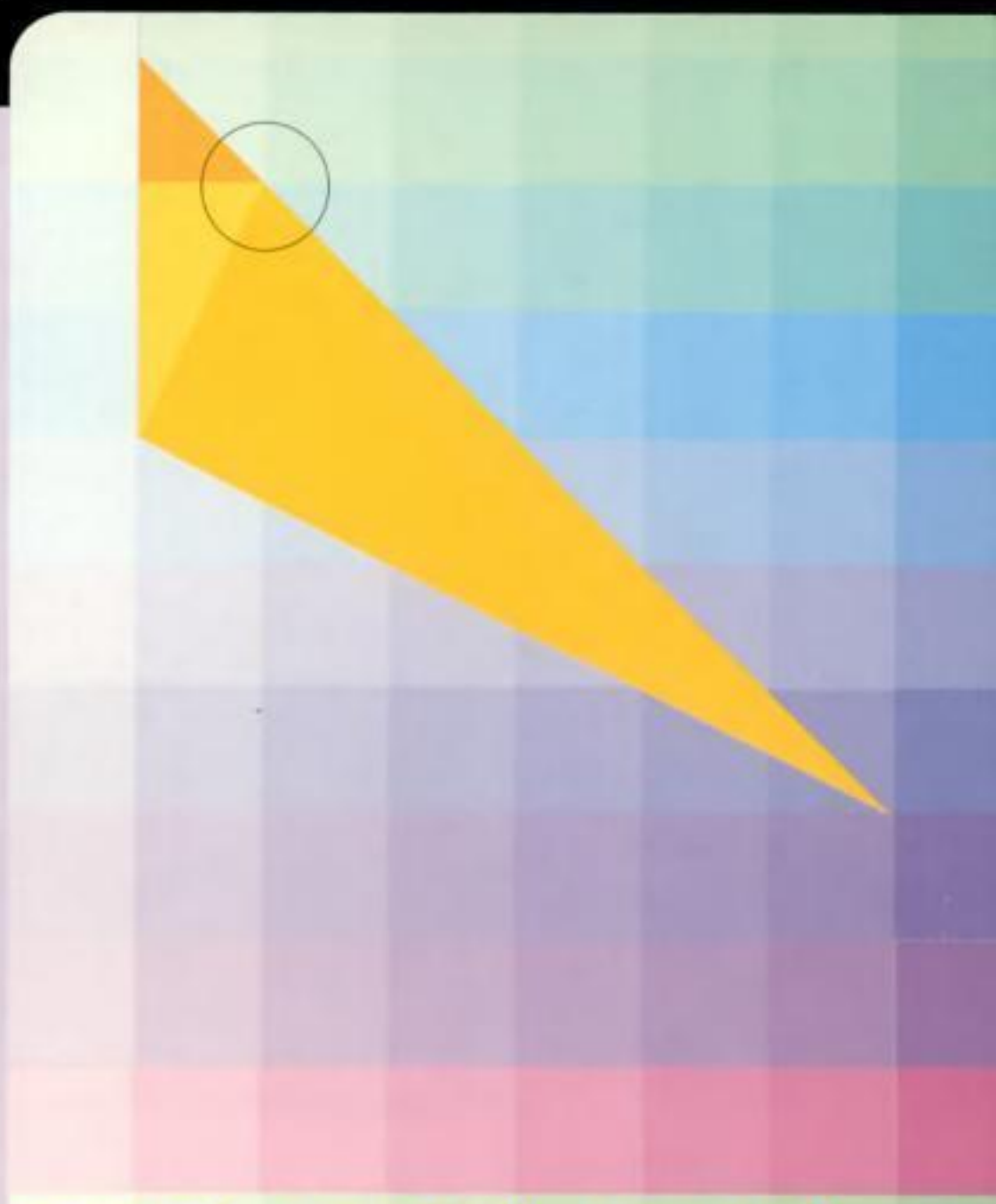
UNIVERSITAT JAUME·I

Manual de matemáticas para preparación olímpica

Cristóbal Sánchez-Rubio
Manuel Ripollés Amela



UNIVERSITAS

$$\arctg 1 + \arctg 2 + \arctg 3 = \pi$$

Copyrighted material

BIBLIOTECA DE LA UNIVERSITAT JAUME I. Dades catalogràfiques

SÁNCHEZ-RUBIO GARCÍA, Cristóbal

Manual de matemáticas para preparación olímpica / Manuel Ripollés Amela, Cristóbal Sánchez-Rubio García. — Castelló de la Plana : Publicacions de la Universitat Jaume I, D.L. 2000

p. : gràf. ; cm. — (Universitas ; 7)

ISBN 84-8021-319-1

1. Matemàtica - Problemes, exercicis, etc. I. Sánchez-Rubio, Cristóbal, coaut. II. Universitat Jaume I (Castelló). Publicacions de la Universitat Jaume I, ed. III. Títol. IV. Sèrie

51(07)

Aquesta publicació no pot ser reproduïda, ni totalment ni parcialment, ni enrregistrada en, o transmesa per un sistema de recuperació d'informació, en cap forma ni per cap mitjà, sia fotomecànic, fotoquímic, electrònic, per fotocòpia o per qualsevol altre, sense el permís previ dels editors.

© Del text: Cristóbal Sánchez-Rubio García y Manuel Ripollés Amela, 2000

© De la present edició: Publicacions de la Universitat Jaume I, 2000

Edita: Publicacions de la Universitat Jaume I. Servei de Comunicació i Publicacions
Campus del Riu Sec. Edifici Rectorat i Serveis Centrals. 12071 Castelló de la Plana
Tel. 964 72 88 19. Fax 964 72 88 32
http://sic.uji.es/publ e-mail: publicacions@uji.es

ISBN: 84-8021-319-1

Depósito legal: Z-2535/2000

Impresión: INO Reproducciones, S.A.

Copyrighted material

ÍNDICE

PRÓLOGO 15

INTRODUCCIÓN 17

I. NÚMERO NATURAL. MÉTODOS DE INDUCCIÓN - SISTEMAS DE NUMERACIÓN .. 19
- Método de inducción matemática 21
- División exacta 23
- División entera 23
- Sistemas de numeración 24
- Cambio de base 25
- Numeración con cifras mínimas (positivas y negativas) 25
- Extensión a números racionales 26
- Complemento aritmético 27

II. DIVISIBILIDAD 29
- Divisores y múltiplos comunes 31
- Números primos y compuestos 33
- Criba de Eratóstenes 34
- Fórmulas para obtener números primos 35
- Divisibilidad por descomposición factorial 35
- Obtención de todos los divisores del número 35
- Descomposición polinómica 36
- Descomposición de factoriales en factores primos 37
- Divisibilidad de factoriales 38

III. CONGRUENCIAS. RESTOS POTENCIALES - CRITERIOS DE DIVISIBILIDAD 39
- Operaciones con congruencias 41
- Sistemas de números incongruentes 42
- Teorema de Euler-Fermat 43
- Teorema pequeño de Fermat 43
- Indicador de un número m 43
- Congruencia de Euler 44
- Números asociados respecto al módulo m 45

Teorema de Wilson 45
Ecuaciones polinómicas módulo p (primo) 46
Teorema de Lagrange 46
Teorema del resto chino 47
Restos potenciales de n respecto al módulo m 48
Raíces primitivas 50
Criterios prácticos de divisibilidad 51
Prueba de operaciones aritméticas 53

IV. GRUPOS FINITOS. CLASES DE RESTOS. CUADRADOS LATINOS Y MÁGICOS 55
Estructuras algebraicas 57
Propiedades de las operaciones 58
Elementos notables 58
Operación compatible con una relación de equivalencia 59
Ley de composición cociente 59
Tablas de la suma y el producto en Z/m 59
Estructura algebraica 60
Homomorfismos 61
Grupos 61
Propiedades del grupo 62
Subgrupos 62
Teorema de caracterización 62
Subgrupo intersección y subgrupo engendrado 63
Grupos de tipo finito y grupos monógenos 64
Clases adjuntas a un subgrupo. Subgrupos normales o invariantes 64
Grupos de sustituciones 65
Grupos finitos 66
Orden de un subgrupo. Teorema de Lagrange 66
Grupos cíclicos 67
Anillos 68
Cuerpos 68
Característica de un cuerpo 69
Cuadrados latinos 69

V. ECUACIONES DIOFÁNTICAS 77
Teorema de Bézout 80
Teorema de existencia 80
Soluciones particulares y solución general de ecuaciones lineales homogéneas 81
Solución de ecuaciones no homogéneas 82
Métodos del Algoritmo de Euclides y el de Cumulantes 85
Cumulantes 87
Soluciones enteras naturales. Procedimiento de «reparto en cascada» 88
Sistemas de ecuaciones lineales 89
Resolución de sistemas lineales diofánticos 89

Copyrighted material

Teorema de existencia de soluciones enteras en sistemas lineales 90
Ecuaciones diofánticas no lineales 91
Ecuación pitagórica 91
Método habitual para ecuaciones diofánticas homogéneas de segundo grado ... 92
Triángulos de lados enteros 93
Ecuación de Fermat 93
Ecuaciones no homogéneas de segundo grado. Ecuación de Pell 93
Algoritmo de fracciones continuas 95
Ecuaciones en congruencias 97

VI. PROGRESIONES 99
Progresiones aritméticas ordinarias 101
Progresiones geométricas ordinarias 102
Progresiones hipergeométricas 103
Convergencia de series geométricas, hipergeométricas y telescópicas 104
Algoritmo de sumas sucesivas 106
Algoritmo de diferencias sucesivas 107
Progresiones aritméticas de orden superior 108
Método de coeficientes indeterminados para el cálculo de u_n y S_n 110
Sucesiones de potencias n^k 111
Método constructivo para el cálculo de a_n y S_n 112

VII. SUCESIONES RECURRENTES 115
Suma de n términos en sucesiones recurrentes 121
Fórmula del término general y de la suma de n términos 122

VIII. POLINOMIOS Y ECUACIONES POLINÓMICAS 127
Polinomios reales y complejos 129
Método de los coeficientes indeterminados 129
División en línea y división sintética 130
Relaciones de Cardano-Vieta 132
Máximo común divisor de polinomios 133
Teorema de Bézout 133
Teorema fundamental del álgebra 134
Anulación del segundo coeficiente por traslación del origen 134
Resolución de ecuaciones polinómicas mediante radicales 135
Polinomios con coeficientes reales 137
Estimación de cotas entre las que oscilan los ceros reales de un polinomio 138
Teorema de Bolzano 139
Ecuaciones reducibles a cuadráticas 140
Ecuaciones recíprocas o simétricas 140
Aplicaciones 143

IX. COMBINATORIA 147
Variaciones 149

Copyrighted material

Variaciones con repetición 149
Permutaciones 150
Permutaciones circulares 150
Inversiones y paridad de una permutación 150
Permutaciones con repetición 151
Combinaciones 152
Combinaciones con repetición 152
Números combinatorios 154
Relaciones entre números combinatorios 155
Triángulo de Pascal 155
Triángulo de Tartaglia 156
Productos de binomios 157
Potencia de un binomio 158
Potencia de un polinomio 158
Suma de potencias de números naturales 159
Binomio de Vandermonde 160
Sustituciones entre n elementos 160
Producto de sustituciones 161
Sustituciones conmutables 162
Sustituciones circulares. Ciclos 162
Descomposición en ciclos 163
Descomposición en transposiciones 163
Potencias de una sustitución 164
Grupos y subgrupos de sustituciones. Grupo Simétrico. Grupo Alternado. Grupo Cíclico 164
Teorema fundamental (LAGRANGE) 165
Tríadas de Steiner 166
La regla aditiva 167
La regla multiplicativa 168
El principio de Dirichlet o del Palomar 169
Elegir un modelo 170

X. DESIGUALDADES 173
Desigualdades clásicas 175
1. Desigualdad de Cauchy-Schwarz 175
2. Desigualdad de Minkowski 176
3. Desigualdad triangular 176
4. Series de fracciones desiguales 176
5. Desigualdad de Bernoulli 177
6. Desigualdades con las medias 177
Desigualdades geométricas 180
Desigualdades con los lados 181
Desigualdades con los ángulos 186

Copyrighted material

XI. NÚMEROS COMPLEJOS 193
Definición 198
Interpretación geométrica. Módulo y argumento de un número complejo 198
Forma trigonométrica de un complejo 199
Razones trigonométricas de ángulos múltiples 200
Raíces n-ésimas de un número complejo 202
Raíces primitivas de la unidad. Polinomios ciclotómicos 203
Exponencial compleja. Fórmula de Euler 206
Complejos y geometría 208
Polígonos regulares y números complejos 212
XII. CONSTRUCCIONES ELEMENTALES CON REGLA Y COMPÁS 217
Aritmética con regla y compás 219
Media proporcional 221
Raíz cuadrada 221
Resolución gráfica de la ecuación de segundo grado 221
Mediatriz, bisectriz y tangente por un punto a una circunferencia 223
Tangentes comunes a dos circunferencias 224
Tangentes interiores 224
Tangentes exteriores 224
Sección áurea de un segmento 225
XIII. ÁNGULOS EN LA CIRCUNFERENCIA 227
Ángulo inscrito 229
Ángulo semiinscrito 230
Ángulo exterior 231
Ángulo interior 231
Cuadrilátero inscriptible 232
Cuadrilátero circunscriptible 233
Polígonos regulares 233
Relaciones métricas en cualquier polígono regular 234
Teorema de Tolomeo 236
XIV. PUNTOS NOTABLES EN EL TRIÁNGULO Y PRIMERAS RELACIONES MÉTRICAS 239
Mediatrices. Circuncentro 241
Alturas. Ortocentro 242
Bisectrices: Incentro 242
Exincentros 242
Triángulo órtico 244
Medianas. Baricentro 244
Recta de Euler 245
Recta de Simson 246
Cuadrado de un lado de un triángulo 246
Suma y diferencia de los cuadrados de dos lados de un triángulo 247
Teorema de Stewart 248
Teorema de Ceva 249

Copyrighted material

XV. RELACIONES MÉTRICAS EN LA CIRCUNFERENCIA 251
Potencia de un punto respecto de una circunferencia 253
Eje radical de dos circunferencias 254
Construcción del eje radical 255
Centro radical de tres circunferencias 256
Circunferencias ortogonales 256
Haz de circunferencias 257
Haces ortogonales 258

XVI. RELACIONES MÉTRICAS EN EL TRIÁNGULO 261
La circunferencia de los nueve puntos 263
Propiedad métrica de las bisectrices 264
Cálculo de las bisectrices 266
Segmentos determinados en los lados por las circunferencias inscrita y exinscrita 267
Radios de las circunferencias inscrita y exinscrita 268
Cálculo de las medianas 269
Cálculo de las alturas y del área 269
Radio de la circunferencia circunscrita 270
Teorema de Euler 270
Teorema de Morley 271
Teorema de Napoleón 273

XVII. LOS MOVIMIENTOS EN EL PLANO 275
Puntos y elementos dobles 277
Traslaciones 278
Giros 279
Simetría central 279
Simetría axial 280
Producto de movimientos 280
Producto de traslaciones 280
Producto de giros del mismo centro 280
Producto de dos simetrías axiales 281
Producto de dos giros de diferentes centros 282
Producto de traslación por giro 283
Movimientos directos e inversos 283
Reflexión-deslizamiento 284
Congruencia 284
Problema de Fagnano 287
Problema de Fermat 288

XVIII. LA HOMOTECIA Y LA SEMEJANZA 291
Homotecia 293
Ecuaciones de la homotecia 295
Producto de homotecias del mismo centro 295

Copyrighted material

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

PRÓLOGO

Comenzaré con una breve presentación de los responsables de este texto. Los autores de este libro, Cristóbal Sánchez-Rubio y Manuel Ripollés son profesores de matemáticas de los IES Penyagolosa y Ribalta de Castellón, respectivamente, y además de su docencia a los estudiantes de bachillerato, dedican buena parte de su tiempo a prepararlos para que puedan presentarse con más opciones a la Fase Local de la Olimpiada Matemática, así como a otras pruebas de Matemáticas, la prueba Canguro entre ellas. También gustan de plantear ejercicios cada semana a los estudiantes de su centro. Además han publicado, en prestigiosas revistas, numerosos problemas originales, los cuales están ubicados sobre todo en el campo de la geometría clásica, especialidad en la que los autores son especialmente brillantes. Algunos de sus ejercicios originales aparecen en este libro.

Esta tarea de preparación que vienen realizando desde hace varios años, junto a su gran interés en el planteamiento y resolución de nuevos problemas les ha llevado a la redacción de este ejemplar que ahora podemos disfrutar. En él se tratan, con rigor, todos los apartados necesarios para una buena preparación olímpica, matemáticamente hablando.

Es una de las pocas obras que existen en nuestro país de preparación olímpica, que no sean obras de recopilación de problemas olímpicos ya planteados en anteriores olimpiadas, nacionales o internacionales. El libro contiene además, prácticamente todos los resultados teóricos necesarios para poder abordar una pruebas de la olimpíada con un mínimo de garantías.

Sabida es la dificultad de conocer todos los resultados matemáticos útiles para la resolución de los problemas planteados en olimpiadas, y más difícil todavía es saber aplicarlos correctamente en cada caso. Este es el mayor obstáculo que debe salvar el estudiante olímpico, y eso es precisamente lo que intenta medir la olimpiada, la capacidad de raciocinio lógico conjugada con los resultados teóricos adecuados.

Copyrighted material

En esta publicación aparecen todos los tópicos matemáticos necesarios y constituye por tanto una gran ayuda para una preparación olímpica adecuada.

No describiré los contenidos de los diferentes capítulos pues dicha labor consistiría en repasar los contenidos de, prácticamente todas las áreas de la matemática: combinatoria, números complejos, sistemas de numeración, etc., pero sí cabe destacar los capítulos dedicados a la geometría clásica, cuyos resultados no se imparten en las enseñanzas medias, ni tampoco en la Licenciatura en Matemáticas, aunque son una parte apasionante de la matemática.

Este libro está destinado a todos aquellos estudiantes que quieran preparar mínimamente su participación en cualquier tipo de prueba o concurso de matemáticas, y especialmente si ésta es la Olimpiada Matemática, para estudiantes del último curso de enseñanzas medias, pero también esta destinado al profesorado de dichos centros que voluntariamente se dedica a preparar a los olímpicos matemáticos. Finalmente, cabe decir que el libro no es sólo específico para la preparación olímpica, sino que, el hecho de que sea una recopilación de resultados matemáticos en casi todos los campos de esta ciencia, la convierte en una obra básica de consulta para estudiantes y matemáticos en general.

El presente libro es una obra que responde a una necesidad que aparece en el momento en que se piensa en resolver problemas de matemáticas que no requieren ninguna técnica específica pero sí el conocimiento teórico de muchos conceptos y resultados que podríamos llamar clásicos y la interconexión entre ellos.

Además también tiene como objetivo el difundir la prueba matemática con mayor prestigio que se realiza actualmente en el país. Las Olimpiadas Matemáticas, que actualmente están en su trigésimo sexta edición, no son un mero concurso en el cual, los participantes buscan una compensación económica. Son un escalón de preparación tan importante, que permite acceder a las titulaciones universitarias con mejor nivel en el campo de la matemática.

Finalmente, decir que, presentar este libro es para mi un honor que agradezco enormemente a los autores pues me permite, en unas líneas, hacer constar el respeto hacia la constante y ardua labor realizada durante años por dos grandes profesionales de la docencia y el estudio de la matemáticas. Siempre es un placer poder contribuir en que salga a la luz un trabajo bien hecho.

TONI GIL
Universitat Jaume I

Copyrighted material

INTRODUCCIÓN

Durante los últimos cursos nos hemos interesado en ayudar a los alumnos que se presentaban a las pruebas de las sucesivas Olimpiadas Matemáticas. Ello nos dio ocasión de comprobar las tremendas lagunas que presentan los programas de matemáticas de enseñanza media en algunas cuestiones de gran incidencia en estas pruebas.

La realidad es que un alumno que sea brillante en las matemáticas de enseñanza media tiene poco que hacer en las pruebas de la Olimpiada Matemática sin una preparación complementaria. Cuestiones básicas como la divisibilidad están apenas hilvanadas en algún curso. Otras, como nociones básicas de teoría de números, ecuaciones diofánticas, congruencias y geometría métrica están completamente ausentes.

Por otra parte, la tendencia de los planes de estudios en los últimos años va claramente encaminada a sustituir los auténticos problemas por una repetición obsesiva de ejercicios para adquirir rutinas. Esta tendencia empapa toda la práctica de la enseñanza de las matemáticas en enseñanza media, desde los libros de texto hasta los tipos de exámenes con ejercicios cada vez más "esperables".

En cada grupo de alumnos hay un porcentaje de ellos (por desgracia pequeño) que tienen lo que podemos llamar gusto por las matemáticas, para los que no existe el problema de la motivación, no se preguntan ¿para qué sirve esto? Para ellos, el reto de intentar resolver un problema y la satisfacción de conseguirlo lo justifica sobradamente con independencia de la utilidad práctica que el problema puede tener.

Algunos profesores pensamos que hay que dedicar un esfuerzo especial a estos alumnos fomentándoles su ilusión por las matemáticas. En esta línea, las Olimpiadas Matemáticas sirven de perfecto banderín de enganche para unas clases de ampliación de matemáticas que, a nuestro juicio, son tan importantes como las clases de recuperación.

Para cualquier acción de este tipo, es fundamental contar con el apoyo del profesorado de matemáticas de los centros de enseñanza media. Con esta idea se impartió un cursillo en el CEP el año 1994. Con el material de aquel cursillo y el recopilado du-

Copyrighted material

rante varios años de las sucesivas pruebas de las Olimpiadas Matemáticas en sus diferentes fases (de distrito, nacionales e internacionales) se ha elaborado este MANUAL DE MATEMÁTICAS PARA PREPARACIÓN OLÍMPICA.

Hemos puesto especial cuidado en no repetir cuestiones que se desarrollan en los temarios vigentes de enseñanza media.

El manual está estructurado en 20 capítulos y dos apéndices de problemas, el primero con 200 problemas de primer nivel (fase de distrito) y el segundo con problemas más difíciles (fases nacional e internacional).

Por supuesto que no pretendemos cubrir todas las cuestiones que pueden interesar a un alumno al que le gustan las matemáticas. Sólo hemos pretendido llenar unos huecos evidentes en la formación de los alumnos de enseñanza media y diseñar un curso de primer nivel que en el futuro podría ser completado.

Este manual va destinado a esos alumnos que citábamos antes a los que no les importa asistir a clases voluntarias de matemáticas fuera del horario lectivo y para los que enfrentarse a un problema es una actividad interesante en sí misma.

También puede ser útil para profesores que preparen a algunos de sus alumnos para las diferentes pruebas y concursos de matemáticas que en los últimos años se están consolidando en nuestro país así como para todas aquellas personas aficionadas a la resolución de problemas.

Parece obvio aclarar que este manual hay que entenderlo como una referencia a la que acudir cuando uno se atasca en la resolución de algún problema. Lo importante es enfrentarse al problema, aquí vale plenamente la afirmación tautológica: «Se aprende a hacer problemas haciendo problemas».

Copyrighted material

I

NÚMERO NATURAL
Métodos de inducción
Sistemas de numeración

Copyrighted material

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

EJERCICIO 3. Demuestra que el producto de cualquier número de factores, sumas de dos cuadrados, es a su vez suma de dos cuadrados.

EJERCICIO 4. Demuestra que:

$$2\,(p+1)^{p+1} < (p+2)^{p+1}$$

(Mejor que por inducción es despejar $2< f(p)$ y aplicar el binomio de Newton).
La fórmula del binomio de Newton se demuestra a su vez por inducción.

EJERCICIO 5. Demuestra que: $n!<\left(\frac{n+1}{2}\right)^n$. (Por inducción, reduciéndolo al anterior).

A veces el método de inducción se sustituye con ventaja por algún artificio imaginativo:

Aquí va bien usar el doble producto n!n!, agrupar factores en orden inverso, y aplicar luego que el producto de dos números de suma fija, 2b, es máximo, si los dos son iguales, bb.

EJEMPLO 1: $12\cdot0 < 11\cdot1 < 10\cdot2 < 9\cdot3 < 8\cdot4 < 7\cdot5 < 6\cdot6$; parejas que suma 12.

En contraposición la suma de dos números de producto fijo b^2 es mínima para $s = b + b$.

EJEMPLO 2: $6 + 6 < 4 + 9 < 3 + 12 < 2 + 18 < 1 + 36$; parejas, todas ellas, de producto 36.

$$(n!)(n!)=(1\cdot n)(2\cdot[n-1])\ldots..(n\cdot1)< \left(\frac{n+1}{2}\cdot\frac{n+1}{2}\right)\cdot\left(\frac{n+1}{2}\cdot\frac{n+1}{2}\right)\ldots\left(\frac{n+1}{2}\cdot\frac{n+1}{2}\right)=$$
$$=\left(\frac{n+1}{2}\right)^{2n}$$

EJERCICIO 6. Demuestra que: $n! > a^n$, desde cierto valor de n, que es función de a.

EJERCICIO 7. Demuestra que la suma de todos los números de la tabla de Pitágoras que contiene los productos de los números 1,2,...,n

$$S=\frac{n^2(n+1)^2}{4}$$

Aquí el artificio que sustituye con ventaja a la inducción es observar que la suma buscada es la de los términos del desarrollo del siguiente producto:

Copyrighted material

$$(1 + 2 + 3 + ... + n).(1 + 2 + 3 + ... + n) = \frac{(n+1)n}{2} \cdot \frac{(n+1)n}{2}$$

DIVISIÓN EXACTA

Si p = m.n se dice que p es múltiplo de m; y que m es divisor de p. Se escribe:

$$p = m \text{ o bien } m \mid p.$$

PROPIEDADES

- Si un número divide a otros dos, divide también a sus múltiplos, a su suma y a su diferencia.
- Si un número divide a la suma o diferencia de dos, y a uno de ellos; también divide al otro.
- La divisibilidad en N es relación de orden parcial (reflexiva, antisimétrica, transitiva y hay parejas de números naturales que no están relacionados en ningún sentido).

DIVISIÓN ENTERA

Si p no es múltiplo de m estará comprendido entre dos términos de la sucesión:

$$m, 2m, 3m, ...$$

Sea $mq < p < m(q + 1)$. Entonces $p = mq + r$, o bien $p = m(q + 1) - r'$.

- q es el cociente entero, y r el resto, *por defecto*, en la división entera de p por m
- q + 1 es el cociente entero y r' el resto, *por exceso*, en la división entera de p por m.

PROPIEDADES

I. El dividendo es mayor que el doble del resto por defecto. (Demostrarlo)
II. Si el dividendo y el divisor se multiplican o dividen por un número, el cociente no varía, pero el resto queda multiplicado o dividido por ese mismo número.

NOTA. La aplicación práctica de la propiedad análoga en la división con decimales es desconocida en lo que al resto se refiere por la mayoria de alumnos brillantes y profesores de matemáticas, debido a que sólo les interesa calcular el cociente y no el resto, que se escribe como entero, sin presentarlo al final con tantos decimales como adquiere el dividendo.

Copyrighted material

Lo mismo ocurre con el resto en el algorítmo de la raíz cuadrada al sacar decimales.

SISTEMAS DE NUMERACIÓN

TEOREMA

Dado un módulo o base $n > 1$, todo número m se descompone de modo único en la forma:

$$m = a + bn + cn^2 + dn^3 + ... + fn^{k-2} + gn^{k-1} + hn^k$$

siendo a, b, c, ...,g, h menores que n.

DEMOSTRACIÓN

Basta dividir reiteradamente por la base n el número m y los sucesivos cocientes obtenidos.

El proceso termina cuando llegamos a un cociente menor que n.

$$m = nq_1 + a$$
$$q_1 = nq_2 + b$$
$$q_2 = nq_3 + c$$
$$.....$$
$$q_{k-2} = nq_{k-1} + f$$
$$q_{k-1} = nq_k + g$$
$$q_k = h < n$$

La expresión del número m en la base n la constituye el conjunto de cifras (todas menores que n) formado por el último cociente y los restos anteriores. Se conviene en hacerlo de la forma:

$$hgf...bca_{(n}$$

que es única al serlo los restos por defecto en la división entera.

Nótese que el valor de cada cifra depende del lugar que ocupa.

La primera por la derecha expresa unidades simples; la segunda unidades de primer orden de valor n; la tercera unidades de segundo orden, de valor n^2; ...

Cuando $n > 10$ las "cifras" superiores a 9 suelen expresarse mediante letras. También puede hacerse por grupos de dos cifras si $10 < n < 101$; de tres cifras si $100 < n < 10001$, ... etc. Ejemplos:

Copyrighted material

356 en base 25 es: $1406_{(25} = 06 + 14 \cdot 25$

23479 en base 60 es: $62119_{(60} = 19 + 21 \cdot 60 + 6 \cdot 60^2$

CAMBIO DE BASE

- De decimal a base n se hace por divisiones sucesivas.
- De base n a base 10 es el valor numérico obtenido por el algorítmo de Ruffini.
- El cambio entre dos bases cualesquiera suele hacerse pasando por la decimal.

NUMERACIÓN CON CIFRAS MÍNIMAS (POSITIVAS Y NEGATIVAS)

En el algoritmo de divisiones para expresar un número en base n, si cada vez que sale un resto r mayor que $\frac{n}{2}$ se tomara por exceso, utilizaríamos sólo la mitad de cifras; pero hay que marcar las que actúan por exceso, con un guión sobre esa cifra.

En base 10, utilizando sólo las cifras 0, 1, 2, 3, 4, 5; el número 374586 sería: $4\bar{3}5\bar{4}\bar{1}4$

En efecto,

$$300000 + (100000 - 30000) + 4000 + 500 + (100 - 20) + (10 - 4) =$$
$$= 400000 - 30000 + 4000 + (1000 - 400) - 20 + 10 - 4 =$$
$$= 400000 - 30000 + 5000 - 400 - 10 - 4$$

Veamos un par de problemas de aplicación:

1) Con una balanza y un juego de pesas de 1, 3, 9, 27,...3^k,.. gramos ¿Es posible pesar cualquier objeto con precisión de 1 gramo?

La respuesta es afirmativa. Basta expresar la cantidad a pesar en base 3 usando las cifras

$$1, 0, -1$$

Las pesas cuya potencia de tres correspondientes a cada "1" se colocan en el platillo de pesas y las correspondientes a cada "–1" en el platillo del objeto considerado.

2) Es un problema clásico, con una versión mas sencilla y otra más difícil.

2*a*) El rey de un país oriental tiene un gobernador en cada una de sus provincias que anualmente le llevan su tributo, consiste en un saco con un número indetermina-

Copyrighted material

do de monedas de oro de p gramos. Uno de los gobernadores hace trampa: todas sus monedas pesan un gramo de menos sin variar forma y tamaño (tienen un burbuja de aire en su interior). Con una balanza de dos platillos y un juego de pesas apto para pesar cualquier cantidad el rey tiene que averiguar en ¡una única pesada! cual es el gobernador que pretende engañarle. No es necesario saber cuántos gobernadores hay ni cuál es el tributo que paga cada uno.

La respuesta es colocar los sacos de cada gobernador en fila y tomar una moneda del primero, dos del segundo, tres del tercero y así sucesivamente hasta terminar los sacos.

Podemos calcular con facilidad la cantidad que deben pesar todas esas monedas:

$$m = p(1 + 2 + 3 + ... + s)) = p\frac{(1+s)s}{2}$$

donde s representa el número de sacos (provincias). Se pesan las monedas y la diferencia d entre el peso m que debería dar si todas las monedas pesasen igual y el peso real indica el número del saco con las monedas modificadas.

2*b*) El mismo planteamiento con varios gobernadores que intentan engañar. Averigua con una sola pesada cuántos y cuáles son los sacos de monedas trucadas en su peso.

La solución consiste en tomar una moneda del primer saco, dos del segundo, cuatro del tercero,...,2^{k-1} del k-ésimo,....hasta terminar los sacos. Ahora el peso debería ser:

$$m = p\left(1 + 2 + 2^2 + 2^3 + ... + 2^s\right) = p\left(2^{s+1} - 1\right)$$

La diferencia d entre m y el peso real da la solución. Expresado d en base 2, las potencias de 2 que tienen coeficiente 1 corresponden a sacos con monedas fraudulentas.

La base dos es especialmente útil por varios motivos: como sólo utiliza dos cifras 0,1 es especialmente apta para el uso interno en ordenadores y en gran número de problemas de configuraciones o estrategia es útil un análisis que implica el conocimiento de la base dos.

EXTENSIÓN A NÚMEROS RACIONALES

Expresiones como $23,432 = 2\cdot 10^1 + 3\cdot 10^0 + 4\cdot 10^{-1} + 3\cdot 10^{-2} + 2\cdot 10^{-3}$ son habituales y las conocemos como números decimales con el significado elemental que

Copyrighted material

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

II

DIVISIBILIDAD

Copyrighted material

DIVISORES Y MÚLTIPLOS COMUNES

DEFINICIONES

Decimos que el número entero a divide al b y escribimos $a|b$, si existe otro entero c tal que:

$$ac = b$$

También se dice en ese caso que a es *divisor* de b, que b es múltiplo de a, y se escribe

Divisores propios de a son los distintos de a, –a, 1 y –1, que lo son de cualquier número a.

Los conceptos de divisor común, a dos o más números, máximo común divisor, múltiplo común y mínimo común múltiplo, son lo que expresan las propias palabras.

PROPIEDADES

- La suma y diferencia de múltiplos de un número es otro múltiplo de ese mismo número.
- Los múltiplos de un múltiplo son sus múltiplos y los divisores de un divisor son sus divisores.

Números primos entre sí son aquellos, dos o más, cuyo m.c.d. es la unidad.

Números primos entre sí dos a dos son aquellos en que cada uno es primo con cualquier otro.

EJEMPLO 1: 6, 10 y 5 son primos entre sí (en conjunto), pero no son primos entre sí dos a dos.

Copyrighted material

PROPOSICIÓN

Los divisores comunes de dos números son divisores comunes del menor de ellos y del resto de dividirlos (ya sea por defecto o por exceso).

DEMOSTRACIÓN: Para la división por defecto: Si $a > b$, $a = bc + r$, entonces $r = a - bc$; luego todo divisor común de dos de ellos es divisor de los tres.

CONSECUENCIA

Cálculo del m.c.d.(a,b) por el *algoritmo de Euclides*: las divisiones sucesivas de a por b, b por el resto r_1, r_1 por el nuevo resto r_2,...etc., conducen a una de resto cero; su divisor r_n es el m.c.d. buscado. Cada cociente se escribe sobre su dividendo dejando lugar al resto siguiente.

EJEMPLO 2: m.c.d.(590, 80) = 10 ya que:

	7	2	1	2
590	80	30	20	10
30	20	10	0	

PROPOSICIÓN

Si dos números se multiplican por k, su m.c.d. queda multiplicado por k. Si los dos se dividen por k, su m.c.d. queda dividido por k.

DEMOSTRACIÓN: Dividendo, divisor y en consecuencia todos los restos del algoritmo de Euclides quedan multiplicados o divididos por ese mismo número k; y en particular también el último divisor, que es el m.c.d.

CONSECUENCIA

Los cocientes de dividir dos números por su m.c.d. son primos entre si.

Notación:

$$\text{m.c.d.}(a,b) = \langle a,b \rangle = D$$
$$a = a'D,\ b = b'D;$$
$$\langle a',b' \rangle = D/D = 1$$

TEOREMA DE EUCLIDES

Si un número m divide al producto de dos factores ab, y es primo con el primero de ellos, entonces divide al segundo.

Copyrighted material

Demostración: $\langle m, a\rangle = 1 \Rightarrow \langle mb, ab\rangle = b \Rightarrow m \mid ab,\ m \mid mb \Rightarrow$
$\Rightarrow m \mid \langle ab, mb\rangle = b$

PROPOSICIÓN

Los múltiplos comunes de a y b son múltiplos de $\frac{ab}{D}$, siendo $D = \langle a, b\rangle$

DEMOSTRACIÓN

Sea $m = ha = kb$, un múltiplo común; $m = ha'D = kb'D \Rightarrow ha' = kb'$; pero $a' \mid kb'$ y es primo con b', luego $a' \mid k \Leftrightarrow k = pa'$. Por tanto:

$$m = pa'b'D = p\frac{a}{D}\frac{b}{D}D = p\frac{ab}{D}$$

CONSECUENCIA

El m.c.m (a,b) es $M = \frac{ab}{D}$ ya que $p\frac{ab}{D}$ es la expresión de los múltiplos comunes, y toma valor mínimo para $p = 1$.

NÚMEROS PRIMOS Y COMPUESTOS

DEFINICIONES

Número primo (primo absoluto) es el que sólo es divisible por sí mismo y por la unidad.

Número compuesto es el que no es primo. Es producto de factores primos: $m = a^{\alpha}.b^{\beta}.c^{\gamma}...l^{\lambda}$.

PROPIEDADES

- Un número primo es primo con sus menores y con todos los que no sean sus múltiplos.
- Si p primo divide al producto abc...hk, divide por lo menos a uno de esos factores.
- La descomposición de un número en factores primos es única.

Estas dos últimas son consecuencia del teorema de Euclides.

Copyrighted material

TEOREMA

La sucesión de números primos es ilimitada.

DEMOSTRACIÓN

Si p fuera el último, el producto de todos los primos más 1: $q = (2.3.5....p) + 1$, sería divisible por $k \leq p$, no unitario; lo que resulta imposible porque k sería divisor de

$$1 = q - (2.3.5...p)$$

PROPOSICIÓN

La sucesión de números primos de la forma $(4m + 1)$ es ilimitada.

DEMOSTRACIÓN

Si $p = 4h + 1$ fuera el último de ellos, entonces llamando P al producto de todos los primos menores o iguales que p resulta que $q = 4P + 1 = 4\cdot(2.3.5.7...[4h + 1]) + 1$ no puede ser primo. Todo divisor primo p' de q debe estar entre los factores de P y resulta ser divisor de $1 = q - 4P$ lo que es imposible.

EJERCICIOS

Demuestra que hay infinitos números primo de la forma $4n + 3$.

Demuestra que hay infinitos números primos de la forma $7n + 6$.

CRIBA DE ERATÓSTENES

Es un método para construir la lista de números primos menores que uno dado $N = k^2$.

- Se escriben el 1(primo) y el 2, seguidos de los enteros impares hasta llegar al N.
- Se suprimen los múltiplos del primo 3 que estarán situados de 3 en 3, a partir del $9 = 3^2$.
- Se suprimen los múltiplos restantes de 5 que estarán situados de 5 en 5, a partir del $25 = 5^2$.
- Se prosigue de esa forma suprimiendo los múltiplos restantes de números primos p, que están de p en p, a partir de p^2; hasta haber actuado con todos los primos menores que k.

Por ejemplo en la tabla de primos $p<100$ los últimos suprimidos son los múltiplos de 7, de 7 en 7, desde $7^2 = 49$, 77 y 91 (el 63 ya está suprimido como múltiplo de 3)

Copyrighted material

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

$$S = \frac{a^{\alpha+1} - 1}{a - 1} \cdot \frac{b^{\beta+1} - 1}{b - 1} \cdots \frac{l^{\lambda+1} - 1}{l - 1} \tag{3}$$

Para hallar el producto P de los divisores de m se consideran las n igualdades

$$m = d_1 \cdot d'_1$$
$$m = d_2 \cdot d'_2$$
$$\cdots\cdots\cdots\cdots$$
$$m = d_v \cdot d'_v$$

donde la sucesión $d_1, d_2, \ldots, d_v$ está formada por todos los divisores de m. Entonces la sucesión formada por $d'_1, d'_2, \ldots, d'_v$, también contiene a todos los divisores. Multiplicando miembro a miembro queda:

$$P^2 = m^v \Leftrightarrow P = \sqrt{m^v} \tag{4}$$

DESCOMPOSICIÓN POLINÓMICA

El estudio de los divisores de un número es paralelo a la factorización polinómica. La expresión de un número en una base es un polinomio en las potencias de dicha base.

Frecuentemente se plantea el estudio de los divisores de un número que viene dado como función polinómica de n, o de la variable intermedia 2^n, 3^n, o en general a^n.

Tiene interés recordar utilidades de factorización de polinomios. Y el método de completar cuadrados perfectos.

$x^2 - a^2 = (x - a)(x + a)$

$x^3 - a^3 = (x - a)(x^2 + ax + a^2)$; $\quad x^3 + a^3 = (x + a)(x^2 - ax + a^2)$

$x^4 - a^4 = (x - a)(x^3 + ax^2 + a^2x + a^3)$. También $(x^2 - a^2)(x^2 + a^2) = (x - a)(x + a)(x^2 + a^2)$

$x^5 - a^5 = (x - a)(x^4 + ax^3 + a^2x^2 + a^3x + a^4)$; $x^5 + a^5 = (x + a)(x^4 - ax^3 + a^2x^2 - a^3x + a^4)$

$x^6 - a^6 = (x - a)(x^5 + ax^4 + a^2x^3 + a^3x^2 + a^4x + a^5)$ También: $x^6 - a^6 = (x^2 - a^2)(x^4 + a^2x^2 + a^4)$

$x^4 + x^2 + 1 = x^4 + 2x^2 + 1 - x^2 = (x^2 + 1)^2 - x^2 = (x^2 + 1 + x)(x^2 + 1 - x)$

EJERCICIO 1. Demuestra que $2^{3n} - 1$ es múltiplo de 7, y da resto 7 al dividir por 56, para todo n.

EJERCICIO 2. Resuelve la ecuación $x^5 + x^4 + x^3 + x^2 + x + 1 = 0$.

Copyrighted material

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

DIVISIBILIDAD DE FACTORIALES

I. El factorial de la suma, M = m' + m", es divisible por el producto de factoriales m'!m"! Su demostración se apoya en una muy poco conocida regla de Cauchy para la prueba de la suma en una base cualquiera. (Análisis matemático. Rey Pastor).

II. El producto de m números consecutivos es divisible por m!
Sea p = (a + 1)(a + 2)(a + 3)....(a + m). En virtud de (I) es (a + m)! = a!m!q.
Dividiendo ambos miembros por a!, queda (a + 1).(a + 2)(a + 3)...(a + m) = = m!q c.q.d.

III. (mn)! es divisible por $(m!)^n$
Basta aplicar (I) a mn = m + m + ...+ m.

IV. Teorema de Weil: (mn)! es divisible por $(m!)^n.n!$
Demostración:
Se aplica (I) a mn –1 = (mn - m) + (m – 1) da (mn – 1)! = [m(n – 1)]!(m – 1)!q_1, que al multiplicar por (mn) queda en la forma (mn)! = [m(n – 1)]!mnq_1.
Repitiendo esta expresión para n = n, n – 1, n – 2, ...,3, 2, 1 y multiplicando sale el teorema de Weil.

Copyrighted material

III

CONGRUENCIAS
Restos potenciales
Criterios de divisibilidad

Copyrighted material

DEFINICIÓN

a y b son números congruentes, respecto del módulo m, si dan el mismo resto al dividir por m: a = mc + r, b = mq + r. Se escribe a ≡ b (mód. m), o bien a ≡ b (m)

PROPIEDADES

1) La congruencia mód. m es relación de equivalencia en N.
2) Los múltiplos de m son congruentes módulo 0 respecto al módulo m.
3) Si a es primo con m, todo número b ≡ a (m) es también primo con m.

CRITERIO

Condición necesaria y suficiente para que a ≡ b (m) es que a – b sea múltiplo de m

CONSECUENCIAS

1) Si a ≡ b (m) también ah ≡ bh (mh), y recíprocamente.
2) Si a ≡ b (p), y a ≡ b (q); también a ≡ b (m), siendo m = m.c.m. (p,q).

OPERACIONES CON CONGRUENCIAS

Para simplificar las expresiones, a veces no se menciona el módulo m, que se sobreentiende.

1. Sumando, restando o multiplicando dos congruencias resulta otra congruencia.
2. Sumando, restando o multiplicando un número a una congruencia, sale otra.
3. Multiplicando miembro a miembro dos congruencias, resulta otra congruencia.
4. Los miembros de una congruencia se pueden elevar a la misma potencia:

Copyrighted material

$$a \equiv b\ (m) \Rightarrow a^n \equiv b^n\ (m)$$

5. Si p(x) es un polinomio con coeficientes enteros y $a \equiv b$ entonces $p(a) \equiv p(b)$.

6. Si $a \equiv b\ (m)$, y p es primo con m, entonces $\frac{a}{p} \equiv \frac{b}{p}\ (m)$.

Demostración:

$a - b = mh$; $a = pa'$, $b = pb' \Rightarrow a - b = p(a' - b') = mh = mph'$; ya que si p divide a (mh) y es primo con m, por el teorema de Euclides, ha de dividir a h.

Por tanto: $a' - b' = mh' \Leftrightarrow a' \equiv b'\ (m)$.

7. Si $a \equiv b\ (m)$ y $a = ka'$, $b = kb'$, pero k no es primo con m; entonces k divide a $m = km'$, y se obtiene otra congruencia dividiendo los tres números (a, b, m) por k: $a' \equiv b'\ (m')$.

8. Se pueden dividir las congruencias $a \equiv b\ (m)$ y $h \equiv k\ (m)$, si h y k son primos con m, además de ser, a divisible por h, y b divisible por k.

SISTEMAS DE NÚMEROS INCONGRUENTES

Sistema de números incongruentes (mód.m) son varios números que dan resto distinto mód m.

Un sistema de números incongruentes tiene a lo sumo m elementos, con restos menores que m.

Sistema completo de números incongruentes mód.m: m números con resto distinto mód. m

El sistema completo más sencillo de números incongruentes mód.m es:

$$0, 1, 2, 3, ..., (m - 1).$$

TEOREMA 1

Si los términos a_1, a_2, ... de un sistema de números incongruentes mód. m se multiplican por n, primo con m, y se les suma o resta un número h, se obtiene otro sistema incongruente mód. m $a_1 \pm h$, $a_2 \pm h$, ... ; que será sistema completo si también lo era el sistema inicial.

En efecto,

$a_i n + h$ es congruente con $a_j n + h$ si y sólo si $(a_i - a_j)n \equiv 0$ (mód.m) si y sólo si $a_i - a_j$

Copyrighted material

TEOREMA DE EULER-FERMAT

Si p es primo y n cualquier número, no divisible por p

$$n^{p-1} \equiv 1 \ (p) \qquad (1)$$

En efecto, {0, 1, 2, 3, ..., p – 1} y {0n, 1n, 2n, 3n, ...,(p – 1)n} son sistemas completos de números incongruentes mód p. Como 0 ≡ 0n, entonces:

$$1\cdot 2\cdot 3\cdot \ldots \cdot (p-1) \equiv 1n\cdot 2n\cdot 3n\cdot \ldots \cdot (p-1)n$$

y puesto que (p – 1)! es primo con p, puede dividirse por él la congruencia anterior y queda la de Fermat.

TEOREMA PEQUEÑO DE FERMAT

Si p es primo y n entero se tiene: $n^p \equiv n \ \ (p)$

En efecto, si p no es divisor de n se reduce al teorema anterior. Si p es divisor de n ambos miembros son congruentes con 0 módulo p.

INDICADOR DE UN NÚMERO m

DEFINICIÓN: Es el número, φ(m), de números primos con m, no superiores a m.

Conviniendo que 1 es primo consigo mismo, admitiremos también que φ(1) = 1

En virtud del teorema 1, en una progresión aritmética de m términos, cuya razón es prima con m, el número de términos que son primos con m es el indicador de m, φ(m).

Daremos sin demostrar la siguiente fórmula para φ(m):

$$\varphi(m) = m\prod_{p|m}\left(1-\frac{1}{p}\right) \qquad (*)$$

donde el producto se extiende a todos los primos p que dividen a m.

PROPIEDADES

1) El indicador de un número primo p es φ(p) = p – 1 (2)

2) Si p primo, entonces $\varphi(p^\alpha) = p^{\alpha-1}\varphi(p) = p^{\alpha-1}(p-1)$ (3)

En efecto: en la sucesión 1,2,3, ..., p^α los únicos no primos con p^α son p, 2p, 3p, ..., ($p^{\alpha-1}$ p). por tanto los que quedan $p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1)$ son los primos con p^α menores que él.

Copyrighted material

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

También lo son na_1, na_2, na_3,..., $na_{\varphi(m)}$. Sus restos mód. m coinciden, salvo el orden, en los dos sistemas. Sus productos son por tanto congruentes. módulo m:

$$na_1 \cdot na_2 \cdot na_3 \cdots na_{\varphi(m)} \equiv a_1 \cdot a_2 \cdot a_3 \cdots a_{\varphi(m)} \ (m)$$

y dividiendo por $a_1 \cdot a_2 \cdot a_3 \cdots a_{\varphi(m)}$, queda $n^{\varphi(m)} \equiv 1\ (m)$.

La congruencia de Fermat es caso particular de la de Euler ya que si m es primo

$$\varphi(m) = m\text{-}1$$

NÚMEROS ASOCIADOS RESPECTO AL MÓDULO m

DEFINICIÓN

Dos enteros n y k se dicen asociados respecto al módulo m cuando $nk \equiv 1\ (m)$.

Puesto que 1 es primo con m también lo es nk y por tanto n. La congruencia de Euler permite hallar el asociado de n módulo m: $nk \equiv n^{\varphi(m)} \equiv 1\ (m)$; y por tanto $k \equiv n^{\varphi(m)-1}\ (m)$

Si n es primo con el módulo m, tiene un asociado y sólo uno, inferior a m.

TEOREMA DE WILSON

Si el módulo p es primo, entonces los únicos números del sistema de incongruentes

$$1, 2, 3, ..., (p-1)$$

que resultan ser asociados de si mismo, son: 1 y p – 1.

En efecto:

$$a^2 \equiv 1\ (p) \Rightarrow (a + 1)(a - 1) \equiv 1\ (p)$$

lo que exige $(a - 1) = p$, o $(a + 1) = p$, luego $a = 1$ o $a = p - 1$.

CONSECUENCIA

Congruencia de Wilson: p es primo si y sólo si $(p - 1)! + 1 \equiv 0\ (p)$.

En efecto, $2 \cdot 3 \cdot \ldots \cdot (p-2) \equiv 1\ (p)$ porque cada uno de esos factores tiene otro que es su asociado.

Multiplicando por (p – 1), se obtiene: $(p-1)! \equiv (p - 1)\ (p)$ con lo que

$$(p - 1)! + 1 \equiv 0\ (p)$$

Copyrighted material

La congruencia de Wilson es una de las escasas caracterizaciones de los números primos.

$$p \text{ primo} \Leftrightarrow (p-1)! \equiv (p-1)\,(p) \Leftrightarrow (p-2)! \equiv 1\,(p)$$

ECUACIONES POLINÓMICAS MÓDULO P (PRIMO)

El teorema fundamental del álgebra establece que para un polinomio f de grado n existen a lo sumo n raíces. Si la ecuación es en congruencias, no existe en general un resultado análogo. Sin embargo, cuando el módulo es un número primo p se cumple el siguiente teorema.

TEOREMA DE LAGRANGE

Dado un número primo p, y el polinomio $f(x) = c_0 + c_1x + \ldots\ldots + c_nx^n$ con coeficientes enteros en que c_n no sea múltiplo de p, entonces: $f(x) \equiv 0\,(p)$ tiene a lo sumo n soluciones.

Se demuestra por inducción sobre el grado n de f(x).

Para n = 1, resulta cierto. La ecuación $c_1x + c_0 = 1\,(p)$ tiene solo una solución, al ser c_1 primo con p.

Supongamos el resultado cierto para grado n – 1 y veámoslo para grado n.

Si $f(x) = 0\,(p)$ tuviera n + 1 soluciones $x_0, x_1, \ldots\ldots x_k$; entonces:

$$f(x) - f(x_0) = c_1(x - x_0) + \ldots\ldots + c_n(x^n - x_0^n) = (x - x_0)g(x)$$

donde g(x) tiene grado n – 1, y como

$$f(x_k) - f(x_0) = (x_k - x_0)g(x_k) \equiv \quad 0 \quad (p)$$

si $k \neq 0$, $x_k - x_0$ no es congruente con 0 módulo p, luego ha de ser $g(x_k) \equiv 0\,(p)$ para k = 1,2...n, en contradicción con la hipótesis de que grado de $g(x) \equiv n - 1$.

Consecuencias del teorema de Lagrange:

1. Dado un número primo p, sea $f(x) = c_0 + c_1x + \ldots\ldots + c_nx^n$ un polinomio de grado n con coeficientes enteros. Entonces, si la congruencia: $f(x) \equiv 0\,(p)$ tiene más de n soluciones, cada coeficiente de f es divisible por p.

Copyrighted material

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

es la solución del sistema de congruencias ya que para $i \neq k \Rightarrow M_i \equiv 0\ (m_k)$ mientras que para $i = k$ se tiene: $b_k M_k M'_k \equiv b_k \cdot 1 \equiv b_k\ (m_k)$ por tanto:

$$x \equiv b_k\ (m_k) \text{ para } k = 1,2,.....r$$

En cuanto a la unicidad módulo M, si hubiese dos soluciones x, y sería $x \equiv y\ (m_k)$ para cada k y como los m_k son primos entre sí dos a dos resultaría $x \equiv y\ (M)$.

EJEMPLO 2: Encontrar un número que dividido entre 2, 3, 5, y 7 dé como restos 1, 2, 3, y 4. Claramente equivale a resolver el sistema:

$$x \equiv 1\ (2)$$
$$x \equiv 2\ (3)$$
$$x \equiv 3\ (5)$$
$$x \equiv 4\ (7)$$

Con la notación usada en la demostración se tiene: $M = 2 \cdot 3 \cdot 5 \cdot 7 = 210$

$$M_1 = 3 \cdot 5 \cdot 7 = 105 \quad M'_1 = 1$$
$$M_2 = 2 \cdot 5 \cdot 7 = 70 \quad M'_2 = 1$$
$$M_3 = 2 \cdot 3 \cdot 7 = 42 \quad M'_3 = 3$$
$$M_4 = 2 \cdot 3 \cdot 5 = 30 \quad M'_4 = 4$$

$$x = 1 \cdot 105 \cdot 1 + 2 \cdot 70 \cdot 1 + 3 \cdot 42 \cdot 3 + 4 \cdot 30 \cdot 4 = 1103$$

El resultado se extiende fácilmente a un sistema:

$$\begin{aligned} &a_1 x \equiv b_1 \quad (m_1) \\ &a_2 x \equiv b_2 \quad (m_2) \\ &\cdots\cdots\cdots\cdots \\ &a_r x \equiv b_r \quad (m_r) \end{aligned} \qquad \text{con } < a_k, m_k >= 1 \quad (k = 1,2,....,r)$$

En efecto, por la hipótesis $<a_k,m_k> = 1$, existe para cada a_k un entero c_k tal que $<a_k,c_k> = 1$.

$$a_k x \equiv b_k\ (m_k) \Leftrightarrow a_k c_k x \equiv b_k c_k\ (m_k) \Leftrightarrow x \equiv b_k c_k\ (m_k)\ (k = 1,2,....r)$$

lo que nos lleva al caso anterior.

RESTOS POTENCIALES DE N RESPECTO AL MÓDULO m

DEFINICIÓN: Son los restos (mód.m) de sus potencias sucesivas

Copyrighted material

El cálculo se hace por recurrencia: dado el resto r_i, su siguiente resto potencial es $n.r_i$ mód. m

$$n^0 = 1 = r_0,\quad n^1 = n\cdot 1 \equiv r_1,\quad n^2 \equiv nr_1 \equiv r_2,\quad n^3 \equiv nr_2 \equiv r_3,\quad n^4 \equiv nr_3 \equiv r_4,\ldots$$

Si n es la base del sistema de numeración la ley de formación de los restos potenciales mód m permite determinar el criterio de divisibilidad por m, para los números escritos en esa base n.

En ocasiones interesa tomar por exceso los restos, si son mayores que la mitad del módulo m.

Ejemplo	n = 10	m = 7	Restos	1, 3, 2, 6, 4, 5, 1, ...	1, 3, 2, $\bar{1}$, $\bar{3}$, $\bar{2}$, 1, ..	
		m = 9		1, 1, ...		(8)
		m = 11		1, 10, 1, ...	1, $\bar{1}$, 1, $\bar{1}$,.1, ...	

El orden g del primer resto que repite valor 1, se llama gaussiano de n respecto al mód. m

PROPOSICIÓN: En el cálculo de los restos potenciales pueden producirse tres casos.

CASO 1: El módulo m contiene únicamente factores primos de n.

Los restos potenciales resultan todos nulos a partir de uno de ellos (sea el de orden k)

Un número es divisible por m si lo es el formado por las k cifras de su derecha.

EJEMPLO 3

$$n = 10 = 2\cdot 5 \qquad m = 250 = 2\cdot 5^3 \qquad n^3 = 1000 \equiv 0 \text{ (mód.250)}$$

CASO 2: El módulo m no contiene ninguno de los factores primos de la base n.

Los restos potenciales de forman una sucesión periódica cuyo número de términos es el gaussiano g de m. Las únicas potencias que dan resto 1 son las de exponente múltiplo de g.

En efecto: al ser m primo con n debe repetirse alguno de los restos 1, 2, 3, ..., (m – 1)

Si $n^{h+k} \equiv n^h\ (m) \Rightarrow n^k \equiv 1\ (m)$ y la serie completa de restos incongruentes (mód.m) es:

$$n^0 = 1,\ n^1,\ n^2,\ \ldots,\ n^{g-1} \qquad (9)$$

siendo $n^g \equiv 1$el primero que repite esta congruencia; y g es el gaussiano de n mód m.

Copyrighted material

Las potencias que dan resto 1 son únicamente las de n^g:

$$n^0,\ n^g,\ n^{2g},\ n^{3g},\ \ldots, \tag{10}$$

El resto de otra potencia será $n^x \equiv n^r$, si es $x = gk + r$

EJEMPLO 4

$n = 10 = 2\cdot5$; $m = 7$; Restos potenciales: (1,3,2,6,4,5,1), o bien $(1, 3, 2, \overline{1}, \overline{3}, \overline{2})$

CASO 3: El módulo m contiene factores primos que son de n y otros que no son de n

Los restos potenciales forman una sucesión periódica mixta. El periodo tiene g términos, si g es el gaussiano de n respecto a m´, producto de los factores de m que no son primos con n.

El anteperiodo consta de tantos términos como restos potenciales no nulos de n respecto al módulo m' si ese es el producto de los factores de m que son primos con n.

Ejemplo:

$n = 10 = 2.5$ $m = 180 = 2^2.5.3^2$ Restos: $(1, 10, 100, 100, ...) = (1, 10, \overline{20}, \overline{20}, ...)$

RAÍCES PRIMITIVAS

Proposición: Si p es primo, y n un número no divisible por p, el gaussiano de n (mód.p), primer exponente $g \neq 0$ que hace $n^g \equiv 1$ (mód.p), es divisor de (p-1)

En efecto: Las únicas potencias congruentes con 1 mod p son $n^0,\ n^g,\ n^{2g},\ n^{3g},\ \ldots$; por lo que la congruencia de Fermat $n^{p-1} \equiv 1\ (p)$ implica que sea (p-1) un múltiplo del gaussiano g.

Cuando el gaussiano es precisamente g = (p-1), se dice que n es una *raíz primitiva* de p.

Entonces son distintos los (p – 1) primeros restos potenciales: $n^0,\ n^1,\ n^2,\ \cdots,\ n^{p-1}$ y repiten en cierto orden los posibles restos 1, 2, 3, ...,(p – 2), (p – 1) respecto al módulo p.

EJEMPLO 5

Para hallar las raíces primitivas de 7 se calculan los restos potenciales de 2,3,4,5,6 mód. 7

Copyrighted material

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

Restos potenciales:1,10,0, ...
N = edcba es divisible por m (1000, 8, 125) si lo es cba.
Restos potenciales:1,10,100,0, ..
N = edcba es divisible por m (9,3) si lo es e + d + c + b + a.
Restos potenciales:1,1,1, ...
N = edcba es divisible por m (11) si lo e – d + c – b + a.
Restos potenciales:1, –1,1, –1,...

Criterios en base 9:
N = edcba es divisible por m ($9=10_{(9}$,3) si lo es a.
Restos potenciales:1,0,0, ...
N = edcba es divisible por m (8,4,2) si lo es e + d + c + b + a.
Restos potenciales:1,1,1, ...
N = edcba es divisible por m ($10 = 11_{(9}$) si lo e – d + c – b + a.
Restos potenciales:1, –1,1, –1,...

Criterios en base 7:
N = edcba es divisible por m = $7 = 10_{(7}$ si lo es a.
Restos potenciales:1,0,0, ...
N = edcba es divisible por m (6,3,2) si lo es e + d + c + b + a.
Restos potenciales:1,1,1, ...

Criterios en base 8:
N = edcba es divisible por m ($8 = 10_{(8}$,4,2) si lo es a.
Restos potenciales:1,0,0, ...
N = edcba es divisible por m = 7 si lo es e + d + c + b + a.
Restos potenciales:1,1,1, ...
N = edcba es divisible por m = $9 = 11_{(8}$ si lo e – d + c – b + a.
Restos potenciales:1, –1,1, –1,...

EJERCICIO 5

Hallar el criterio de divisibilidad por (n + 1) en base n; que es siempre el mismo.

EJERCICIO 6

Hallar el criterio de divisibilidad por m, divisor de n – 1, en la base n.

EJERCICIO 7

Hallar el criterio de divisibilidad por m, divisor de n (incluido m = n), en la base n.

Copyrighted material

EJERCICIO 8

Hallar los números, de cifras iguales, que son divisibles por 3.

EJERCICIO 9

Hallar los números, de cifras iguales, que son divisibles por 9.

EJERCICIO 10

Hallar los números, de cifras iguales, que son divisibles por 11.

PRUEBA DE OPERACIONES ARITMÉTICAS

Consiste en repetir las operaciones con las congruencias módulo m, si en el criterio de divisibilidad por m intervienen todas las cifras. La más usual es la prueba del 9, y la del 11.

Son pruebas de carácter negativo. Si la prueba sale mal es necesario repetir la operación; si sale bien se da por buena aunque puede haber errores que se compensen de cara a la prueba.

Prueba del 9: Las congruencias mód. 9 de los datos y resultado se disponen ordenadas en los ángulos de un aspa, se repite con ellos, la operación, y ha de dar un resultado congruente.

Producto de dos números	2825 x 574 = 1621550	Pruebas correctas
Sus congruencias mód. 9:	8 x 7 = 2	8x7 = 56 ≡ 5 + 6 = 11 ≡ 2 (mód. 9)
Sus congruencias mód. 11:	9 x 2 = –4	9x2 = 18 ≡ 8-1 = 7 ≡ –4 (mód. 11)

División entera:	2769965: 4825 = 574 (resto 415)		Pruebas correctas
Módulo 9	8: 1 = 7 (resto 1)	d.c + r = D	1x7 + 1 = 8 ≡ 8 (mód. 9)
Módulo 11	0: 7 = 2 (resto 8)	d.c + r = D	7x2 + 8 = 22 ≡ 0 (mód. 11)

Copyrighted material

IV

GRUPOS FINITOS
Clases de restos
Cuadrados latinos y mágicos

Copyrighted material

ESTRUCTURAS ALGEBRAICAS

Operación o ley de composición interna sobre el conjunto A, no vacío, es una aplicación del conjunto producto, AxA, en A:

$$A \times A \xrightarrow{\cdot} A$$
$$(a, b) \rightarrow a * b$$

(Diremos operación en vez de operación interna)

Notación: En ocasiones usaremos la notación aditiva (a+b) o la multiplicativa (a.b o bien ab).

Parte estable o subconjunto cerrado para una operación interna definida en el conjunto A es un subconjunto C de A si $\forall$ a,b $\in$C, se verifica que a.b $\in$C.

Con ello la operación * de A queda subordinada, restringida, o inducida en C.

EJEMPLO: La suma de N induce una suma también en el conjunto P de los números pares de N.

Ley de composición externa en A, con dominio de operadores en K, es una aplicación

$$K \times A \xrightarrow{\cdot} A$$
$$(k, a) \rightarrow k \bullet a$$

que a la pareja (k,a) le asigna un elemento de A que designaremos por k.a o ka.

EJEMPLO: Si A es el conjunto de funciones reales de una variable real y K el cuerpo de los números reales podemos definir el producto que al par (k, f) asigna la nueva función k.f(x) = k[f(x)]

Copyrighted material

También hay leyes de composición externa del tipo AxA en K, como el producto vectorial, que a una pareja de vectores asigna un elemento que ya no es vector sino número real.

PROPIEDADES DE LAS OPERACIONES

1. Asociativa: si $\forall$ a, b, c $\in$ A es $(a_*b)_*c = a_*(b_*c)$. (Notación: a + a +...+ a = na; a.a.a...a = a^n)

2. Conmutativa: si $\forall$ a, b $\in$ A es $a_*b = b_*a$

3. Distributiva de (o) respecto a (*) si $\forall$ a, b, c $\in$ A es $ao(b_*c) = (aob)_*(aoc)$

Cuando una operación (.) no es conmutativa los pares que cumplen la condición $a_*b = b_*a$ (no todos) se llaman elementos permutables entre sí. Cuando un elemento conmuta con todos los de A es un elemento central de A. La ley (.) es conmutativa si el centro de A para . coincide con el propio A.

ELEMENTOS NOTABLES

Decimos que e es elemento neutro de A, en la operación (.), si $\forall$ a $\in$ A es

$$a_*e = e_*a = a$$

Si la ley es aditiva (multiplicativa) el neutro se llama nulo (unidad) y su signo es el 0 (el 1).

El conjunto A-{e} suele representarse por A* (A sin el elemento neutro de la operación en A).

Se dice que a' $\in$ A es simétrico de a $\in$ A (cuando hay elemento neutro e) si $a_*a' = a'_*a = e$

En la suma, el simétrico de a se llama opuesto de a, y se designa por -a.

En el producto el simétrico de a se llama inverso de a, y se designa por a^{-1}.

Si a tiene simétrico se llama simetrizable, y su simétrico a' también lo es; además: (a')' = a

El elemento c $\in$ A es simplificable o regular, si

$$a*c = b*c \Rightarrow a = b$$

Si todo elemento de A es regular para la ley . se dice . que cumple la ley de simplificación.

Copyrighted material

En esas mismas condiciones la ecuación a.x = b tiene solución única.

Contraejemplo: 75 no es regular en N con la operación mcd, ^,: (75^90) = (75^30) pero 90 ≠ 30

El elemento a es idempotente en la operación ., si cumple que: a.a = a

Una ley es idempotente para un conjunto A si son idempotentes todos sus elementos.

OPERACIÓN COMPATIBLE CON UNA RELACIÓN DE EQUIVALENCIA

La operación ., definida en A, es compatible con la relación de equivalencia ≈ , definida en A, si:

$$\forall\ a, a', b, b' \in A \text{ tales que } (a \approx a' \text{ y } b \approx b') \Rightarrow a \,.\, b \approx a' \,.\, b'$$

EJEMPLO: La suma y el producto en Z son compatibles con la congruencia módulo m; es decir:

$$a \approx a',\ b \approx b' \text{ implican que } (a+b) \approx (a'+b') \text{ y que } (a.b) \approx (a'.b')$$

En efecto: a = a' + m, b=b'+ m, de donde:

$$a + b = a' + b' + \text{y } (a.b) = (a' \,.\, b') + m \text{ cqd.}$$

LEY DE COMPOSICIÓN COCIENTE

La operación . definida en A, y compatible con la relación de equivalencia ≈ , induce o subordina otra operación designada también . en el conjunto de clases o conjunto cociente A/ ≈ .

La ley inducida se llama también ley de composición cociente.

$$[a] + [b] = [a + b] \text{ siendo } [x] \text{ la clase de equivalencia del } x$$

TABLAS DE LA SUMA Y EL PRODUCTO EN Z/m

Veamos como ejemplo las tablas de suma y producto en Z/5={0,1,2,3,4}

Copyrighted material

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

ESTRUCTURA ALGEBRAICA

Llamamos estructura algebraica al ente formado por un conjunto A y una o mas operaciones definidas en él, que cumplen determinadas propiedades características de cada tipo de estructura.

GRUPOIDE es una estructura con una sola operación.

ÁLGEBRA es una estructura con dos operaciones.

RETÍCULO es un conjunto C con dos operaciones (v, ∧) que son las dos idempotentes, conmutativas, asociativas y cumplen la ley de absorción:

$$\forall\ a, b \in C \qquad a \vee (a \wedge b) = a \qquad a \wedge (a \vee b) = a$$

EJEMPLOS

1) N* con mcm y mcd

2) R con máx. y mín.

3) Partes de A con $\cup$ e $\cap$

El retículo es distributivo si cualquiera de las dos operaciones es distributiva respecto a la otra.

El retículo es complementado si tiene dos elementos especiales llamados nulo (0) y universal (U) y a cada elemento $x \in C$ va asociado otro, su complemento $x' \in C$, verificando:

$$x \vee x' = U; \qquad x \wedge x' = 0$$

Un retículo distributivo y complementado se denomina Álgebra de Boole.

Copyrighted material

HOMOMORFISMOS

Una aplicación f entre dos grupoides (A, .) y (B, ⊥) es homomorfismo si es lineal

$$\forall\ a, b \quad \in A, \quad f(a . b) = f(a) \perp f(b) \qquad (1)$$

Se demuestra que la imagen f(A) es una parte estable de B para la operación ⊥ y en consecuencia el homomofismo queda definido entre (A, .) y (f(A), ⊥), que es su imagen homomorfa

El homomorfismo se llama monomorfismo, epimorfismo o isomorfismo, según que la aplicación sea inyectiva, sobreyectiva o biyectiva.

Un homomorfismo de (A,.) en (A,.) es un endomorfismo; y si es biyectivo automorfismo.

EJEMPLO 1. El logaritmo decimal es un isomorfismo de $(R^*_+; \ )$ en (R; +), ya que

$$\log(xy) = \log(x) + \log(y)$$

EJEMPLO 2. La aplicación f: N → C, $f(n) = i^n$ es homomorfismo de (N,+) en (C,); notemos que:

$$f(N) = \{1,-1,i,-i\}$$

EJEMPLO 3. Un automorfismo en (C; +, ¯) es el que asocia a cada complejo su conjugado:

$$a + bi \rightarrow a - bi$$

ya que el conjugado de la suma o del producto de z y z' es la suma o producto de sus conjugados.

GRUPOS

Grupo es la estructura formada por un conjunto G y una operación „ con las propiedades asociativa, existencia de elemento neutro (e) y existencia de simétrico x' para cada elemento x de G.

Si además se cumple la propiedad conmutativa, se trata de un grupo conmutativo o abeliano.

Copyrighted material

En general se suele utilizar notación multiplicativa para los grupos y aditiva para grupos abelianos. La "potencia" de a, de orden n, se denota en tales casos: a.a.a....a = a^n o a + a + a = na.

Orden de un elemento a del grupo (G,.) es el mínimo número natural n tal que a.a..$^{(n}$...a = e

En notación multiplicativa a^n = e. En notación aditiva: na = e (e, elemento neutro).

EJEMPLO 4. En el grupo multiplicativo {1, -1, i,-i}, esos elementos son de orden (1, 2, 4, 4)

EJEMPLO 5. En (Z/(5),) los elementos son { $\bar{1}$, $\bar{2}$, $\bar{3}$, $\bar{4}$ } y sus órdenes (1, 4, 4, 2), respectivamente.

PROPIEDADES DEL GRUPO

1) El neutro es único.

2) El simétrico de cada elemento x es único.

3) El simétrico del "producto" es "producto" de simétricos en orden contrario: (a . b) ' = b' . a'

4) Todos los elementos son simplificables a . b = a . c implica que b = c

5) Las ecuaciones x * a = b, a * y = b tienen solución en (G, .): x = b.a', y = a'.b

SUBGRUPOS

SUBGRUPO H del grupo (G,.), es un subconjunto H $\subset$ G que con la operación inducida es grupo, por tanto debe verificar:

S0: $\forall$ a, b $\in$ H, a . b $\in$ H (H es parte estable)

S1: La propiedad asociativa es cierta en H $\subset$ G

S2: El elemento neutro e de G está en H

S3: Si a' es el simétrico de a $\in$H entonces a' $\in$H

TEOREMA DE CARACTERIZACIÓN

H, subconjunto no vacío de G, es subgrupo de (G,*) si y sólo si $\forall$ a,b $\in$ H, a.b' $\in$ H (S)

DEMOSTRACIÓN

Necesidad: Si H es subgrupo, la condición (S) es cierta

Copyrighted material

Suficiencia: Suponiendo (S), S1 se cumple por $H \subset G$

S2: $a,a \in H$, $a*a' = e \in H$

S3: $e,a \in H$, $e*a' = a \in H$

S0: $a,b \in H$, $b' \in H$, $a*(b')' = a*b \in H$

Ejemplos:

- Los elementos de la forma 2^n, $n \in Z$ son subgrupo del grupo multiplicativo $(Q^*,\cdot)$
- Las traslaciones o los giros de un mismo centro son subgrupos de los movimientos del plano.
- En el grupo (Z,+) para cada p es subgrupo el conjunto:

$$(p) = pZ = \{0, p, -p, 2p, -2p, ...\}$$

Ejercicio: Demuestra que todo subgrupo de (Z,+) es del tipo pZ anterior (para un $p > 0$, mínimo)

Subgrupos impropios del grupo G son el propio G y {e}, siempre subgrupos en cualquier grupo G.

SUBGRUPO INTERSECCIÓN Y SUBGRUPO ENGENDRADO

PROPOSICIÓN

La intersección $H = \bigcap_{H_i \subset G} H_i$ de subgrupos de G también es subgrupo de G.

DEMOSTRACIÓN: H es no vacío por $e \in H$; si $a, b \in H$, también $a*b' \in H$ como a cada uno de los Hi

PROPOSICIÓN

La unión de subgrupos no es en general subgrupo.

DEMOSTRACIÓN: Basta un contraejemplo. $H = 2Z \cup 3Z$ no es subgrupo de (Z,+) pese a serlo 2Z y 3Z.

H no es cerrado para la suma $2 + 3 = 5 \notin H$

Para subsanar esta aparente deficiencia se define el concepto más amplio de subgrupo engendrado.

PROPOSICIÓN

Dado el grupo (G,+) el conjunto obtenido operando un número finito de veces con elementos de un conjunto C y sus inversos, es subgrupo H, llamado subgrupo engendrado por C.

Copyrighted material

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

Nota: en la definición de determinante de una matriz cuadrada se utilizan conceptos relativos a sustituciones o permutaciones entre índices de filas y columnas: número de inversiones que presenta una permutación, paridad de ese número p, signatura de la permutación que es $(-1)^p$.

GRUPOS FINITOS

G es grupo finito si tiene un número finito de elementos, que llamaremos orden del grupo G.

En tal caso el grupo G es finitamente engendrado al ser el propio G su conjunto generador.

El recíproco no es cierto: (Z,+) no es finito pero si de tipo finito (y monógeno, generado por {1})

ORDEN DE UN SUBGRUPO. TEOREMA DE LAGRANGE

Si (G,*) es grupo finito de orden n y H es subgrupo de G, también H es finito, de orden $m < n$.

En consecuencia también son de orden m las clases adjuntas por la izquierda al subgrupo H . Como esas clases constituyen una partición de G, si son r las clases, ha de ser: $n = m \cdot r$

Por tanto el orden de un subgrupo es divisor del orden del grupo (Teorema de Lagrange).

Salvo isomorfismo son pocos los grupos finitos de un orden dado (no alto) Para hacer el estudio de los posibles grupos de orden menor que siete, y sus isomorfismos, basta confeccionar su tabla y tener en cuenta que:

- El elemento neutro repite las entradas de la tabla
- Los elementos que no son simétricos de si mismo están por parejas.
- Por la regla de simplificación en cada línea están todos los elementos sin poderse repetir.
- En un isomorfismo de grupos la imagen del neutro es neutro y la del simétrico es simétrico.

Copyrighted material

- En particular, el isomorfo del simétrico de sí mismo (ó de otro), tiene esa misma condición.
- Si el orden de G es primo no tiene subgrupos propios y por tanto no hay simétricos de sí mismo.

PROPOSICIÓN

Existen dos tipos de grupos no isomorfos de orden 2, cuatro de orden 6, y sólo uno para los grupos de orden 1, 2, 3 o 5. (Usaremos notación multiplicativa y neutro "e")
Orden 1: (neutro sólo) e e = e
Orden 2: (el neutro y otro a, simétrico de sí mismo) ee = e aa = e
Orden 3: (e; simétricos ab = e (orden primo); por simplificación: aa = b; bb = a)
Orden 4: (e; simétricos ab = cc e; resto por simplificación: ac = ca = b; bc = cb = a)
Orden 4: (e; simétricos aa = bb = cc = e; por simplificación: ab = ba=c; bc = cb = a; ca = ac = b)
Orden 5: (e; simétricos ab = cd = e (orden primo) resto por simplificación).

GRUPOS CÍCLICOS

Un grupo finito se llama cíclico si está engendrado por uno de sus elementos (es monógeno y finito).

Ejemplo: el grupo multiplicativo {1, −1, i, −i} es cíclico engendrado por i o por −i.

PROPOSICIÓN

Un grupo cíclico de orden p, engendrado por g, es de la forma $\{g^h / h = 1, 2,...,p\}$ y el elemento neutro es $e = g^p$ (notación multiplicativa).

CONSECUENCIA: En un grupo finito G, de orden p y elemento neutro e, $\forall g \in G$, es $g^p = e$

PROPOSICIÓN

Un grupo finito de orden primo p, es monógeno, y está engendrado por cualquiera de sus elementos que no sea el neutro e.

DEMOSTRACIÓN: El subgrupo que engendra no es propio (por ser p primo), ni es {e}, luego es el grupo total G.

CONSECUENCIA: Si p es primo, sólo existe un grupo finito de orden p, salvo isomorfismos.

Copyrighted material

Ejemplo: El único grupo de orden 3 es G={ a, b, e } = { a^1, a^2, a^3 } = { b^1, b^2, b^3 } con las correspondencias: b = a^2 = aa, a = b^2 = bb, e = a^3 = aaa = ab = bbb =b^3

ANILLOS

Relación de conceptos conocidos y ampliados:

Anillo (A,+,.), si (A,+) es grupo abeliano y el producto es asociativo y distributivo respecto a +. Anillo unitario (si lo es el producto). Anillo conmutativo (si lo es el producto).

Elementos inversibles en un anillo unitario (forman grupo multiplicativo).

Elementos permutables (respecto al producto) en un anillo no conmutativo.

Reglas de los signos del producto:

$$a.0 = 0.a = 0;\ (-a).b = a(-b) = -(a.b);\ (-a).(-b) = a.b$$

Divisores de cero: elementos no nulos cuyo producto es cero.

Anillo de integridad: sin divisores de cero.

Dominio de integridad: anillo de integridad unitario y conmutativo.

PROPOSICIÓN

El anillo Z/p es dominio de integridad si y sólo si p es primo.

Subanillo de (A,+,·) es B $\subset$ A, si y sólo sí

1) B es subgrupo de (A,+)

2) B es estable para el producto.

Ideal de (A,+,·) es I $\subset$ A, verificando por definición:

1) I es subgrupo de (A,+)

2) $\forall\ i \in I,\ \forall\ a \in A$ es i.a, a.i $\in$ I

Ejemplo (p) = pZ = {múltiplos enteros de p} es ideal del anillo de los enteros.

CUERPOS

Es un anillo (K,+,·), unitario en el que los elementos no nulos son todos inversibles.

Puede considerarse que además ha de ser conmutativo el anillo y hablar de cuerpo no conmutativo en caso contrario. O no considerar conmutativo el anillo, y hablar de cuerpo conmutativo si lo es.

Copyrighted material

PROPIEDADES

- Todo cuerpo es dominio de integridad
- Todo dominio de integridad finito es cuerpo.
- Los únicos ideales de un cuerpo K son K y {0}
- En un cuerpo K, la ecuación $b \cdot x = a$, con $b \neq 0$ y $a, b \in K$, tiene siempre solución única.

PROPOSICIÓN: $(Z/p, +, \cdot)$ es cuerpo si y sólo si p es primo

CARACTERÍSTICA DE UN CUERPO

Sea K un cuerpo, e su elemento unidad y 0 su elemento neutro. Consideremos las siguientes sumas:

$$e, 2e = e + e, 3e = e + e + e, \ldots\ldots, ne = e + e + \ldots + e, \ldots\ldots$$

Si existe un número natural p tal que $pe = 0$ se dice que el cuerpo K es de característica p. En caso contrario se dirá que el cuerpo K es de característica infinita (o bien de característica cero).

La característica de un cuerpo es, pues, el orden de su elemento unidad respecto a la suma.

Son cuerpos de característica infinita Q, R, C. Es de característica p el cuerpo Z/p, si p es primo.

CUADRADOS LATINOS

Dado un conjunto de n símbolos distintos $a_1, a_2, \ldots a_n$; llamaremos cuadrado latino a una disposición de ellos en n filas y n columnas de modo que en cada fila y en cada columna haya uno y sólo uno de ellos. Por ejemplo si n = 4:

a	b	c	d		α	β	γ	δ		aα	bβ	cγ	dδ
b	a	d	c		γ	δ	α	β		bγ	aδ	dα	cβ
c	d	a	b		δ	γ	β	α		cδ	dγ	aβ	bα
d	c	b	a		β	α	δ	γ		dβ	cα	bδ	aγ

El cuadrado de la izquierda es un ejemplo de cuadrado latino con los símbolos {a,b,c,d}; el del centro es otro ejemplo de cuadrado latino con los símbolos {α,β,γ,δ}.

Copyrighted material

El cuadrado de la derecha es la superposición de los otros dos. En él se observa que cada pareja de símbolos aparece una sola vez. Cuando al superponer dos cuadrados latinos ocurre esto, decimos que ambos cuadrados son ortogonales y al cuadrado resultante se le denomina grecolatino.

Los cuadrados latinos y grecolatinos se conocen desde hace muchos años. Euler (1713-1783) los estudió en profundidad e hizo una célebre conjetura que luego expondremos.

La existencia de cuadrados grecolatinos para un orden n dado se mantuvo en principio en el contexto de las curiosidades matemáticas, pero a mediados del siglo XX Fisher demostró su utilidad para el control de experimentos estadísticos, más concretamente en experiencias agronómicas. A nosotros nos interesan por su relación con los cuadrados mágicos que veremos a continuación.

Se llama cuadrado mágico de orden n a una disposición de n^2 números naturales consecutivos (ordinariamente desde el 1 hasta el n^2) en las n^2 posiciones de un encasillado de n filas y n columnas de modo que no se repita ninguno y que las n filas y las n columnas sumen lo mismo.

Veamos primero que la existencia de un cuadrado grecolatino de orden n permite construir un cuadrado mágico del mismo orden.

En efecto, si interpretamos los n símbolos del primer conjunto como cifras en base n (desde 0 a n-1) y lo mismo para las del segundo, el cuadrado grecolatino representa n^2 números diferentes de dos cifras expresados en base n.

Equivale a cambiar ambos conjuntos de símbolos por el conjunto {0,1,2,....n-1}. El cuadrado grecolatino de la página anterior escrito de este modo está colocado a la izquierda:

00	11	22	33
12	03	30	21
23	32	01	10
31	20	13	02

0	5	10	15
6	3	12	9
11	14	1	4
13	8	7	2

1	6	11	16
7	4	13	10
12	15	2	5
14	9	8	3

El carácter de grecolatino asegura la no repetición de números. Comienza en 0 (escrito $00_{(4}$) y termina en n^2-1 (escrito $33_{(4}$). Por tanto están n^2 números consecutivos.

En el cuadrado central se han colocado los mismos números en base 10 (desde el 0 hasta 15) y en el de la derecha se ha sumado 1 a cada celda, con lo que se sitúan en el rango 1....n^2 como suele ser habitual.

Copyrighted material

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

Sea $V = K \times K = \{(a,b) \mid a,b \in K\}$. Como K tiene 5 elementos, V tiene 25, que interpretados como coordenadas de puntos constituyen lo que llamaremos una geometría finita.

Podemos definir "rectas" como los subconjuntos de V soluciones de ecuaciones del tipo ax+by=c, en la que todos los coeficientes y operaciones indicadas se refieren a los de K.

Por ejemplo y = 3x + 2 es una recta que contiene los puntos (0,2); (1,0); (2,3); (3,1) y (4,4).

Puestas las ecuaciones en forma explícita hay 5 valores para la pendiente y otros 5 para la ordenada en el origen. En esta clasificación no están las rectas del tipo x = b, de las que existen otras cinco. En total disponemos de 30 rectas cada una con cinco puntos.

Al ser K cuerpo las propiedades "esperables" entre rectas y puntos son de inmediata comprobación como por ejemplo:

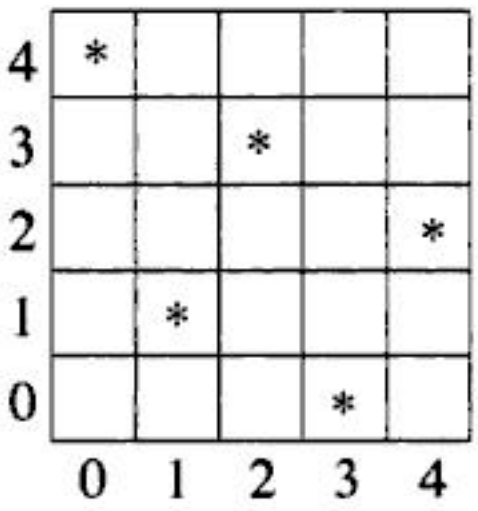
a) Dos puntos distintos definen una única recta.

b) Dos rectas son "paralelas" (no tienen puntos comunes) si y sólo si tienen la misma pendiente y distinta ordenada en el origen.

c) Dos rectas no paralelas se cortan en un único punto.

La representación gráfica de esta geometría inicialmente la haremos en unos ejes clásicos que nos proporcionan una retícula de 25 puntos aislados, es decir entre 2 y 3 no hay nada.

Asociaremos cada valor de la abscisa a una columna y cada valor de la ordenada a una fila, de modo que los 25 puntos de V se corresponde con las 25 celdas de una cuadrado de orden 5.



La figura de la izquierda muestra la representación gráfica que usaremos para nuestra geometría si usamos un símbolo cualquiera, por ejemplo * para un punto. La recta y = 2x + 4 es el conjunto representado en ella correspondiente a los puntos:

{(0,4); (1,1); (2,3); (3,0); (4,2)}

A primera vista se observa que hay un asterisco y sólo uno en cada línea (fila o columna).

Copyrighted material

Por supuesto que no es casualidad: expresa gráficamente el hecho de que la recta dada y = 2x + 4 corta en un único punto a cada una de las rectas y = b (b = 0,1,2,3,4) que son las ecuaciones de las filas (rectas paralelas al eje X). De modo análogo ocurre con las columnas.

Si representamos las cinco rectas de una misma pendiente en la misma gráfica tendremos una representación como la que se muestra en la figura de la derecha para las rectas de la forma y=x+n usando como símbolos a, b, c, d y e para los puntos de las rectas correspondientes a los valores de n 0, 1, 2, 3 y 4 respectivamente.

Evidentemente se obtiene un cuadrado latino ya que cada letra aparece una y sólo una vez en cada fila y en cada columna; por la razón expuesta en el párrafo anterior. No puede haber dos letras distintas en la misma celda ya que dos rectas paralelas no tienen punto comunes. El razonamiento se completa al tener 5 rectas distintas con cinco puntos distintos cada una de ellas llenando el cuadrado de orden 5.

4	e	d	c	b	a
3	d	c	b	a	e
2	c	b	a	e	d
1	b	a	e	d	c
0	a	e	d	c	b
	0	1	2	3	4

Cada valor de la pendiente distinto de 0 (fallaría el razonamiento para las filas) nos proporciona un cuadrado latino. Disponemos entonces de 4 cuadrados latinos, el ya expuesto y los tres restantes correspondientes a las pendientes 2, 3 y 4:

4	e	c	a	d	b
3	d	b	e	c	a
2	c	a	d	b	e
1	b	e	c	a	d
0	a	d	b	e	c
	0	1	2	3	4

4	e	b	d	a	c
3	d	a	c	e	b
2	c	e	b	d	a
1	b	d	a	c	d
0	a	c	e	b	e
	0	1	2	3	4

4	e	a	b	c	d
3	d	e	a	b	c
2	c	d	e	a	b
1	b	c	d	e	a
0	a	b	c	d	e
	0	1	2	3	4

Además, eligiendo dos cualesquiera de entre los cuatro anteriores resultan ortogonales, dado que al representar cada cuadrado latino un haz de rectas paralelas resulta que cada recta de un haz corta a cada recta de otro haz en un punto y sólo en uno, lo que garantiza la ortogonalidad.

Comprobamos así un hecho general: para un orden n dado existen a lo sumo n-1 cuadrados latinos mutuamente ortogonales.

Para que las diagonales también sean mágicas hay que elegir los cuadrados latinos entre los que tengan pendientes distintas de 1 y 4 ya que estos valores son precisamente las pendientes de ambas diagonales.

Copyrighted material

Con este método sólo disponemos de un cuadrado grecolatino que proporcione uno mágico incluyendo ambas diagonales. Hay que partir para ello de los dos latinos asociados a las pendientes 2 y 3.

25	12	4	16	8
19	6	23	15	2
13	5	17	9	21
7	24	11	3	20
1	18	10	22	14

Superponiéndolos, interpretando las letras como cifras en base 5, pasando a base 10 y sumando a todos una unidad se obtiene el cuadrado mágico que se muestra en la figura de la izquierda en el que filas, columnas, diagonales y "paralelas" a las diagonales suman 65.

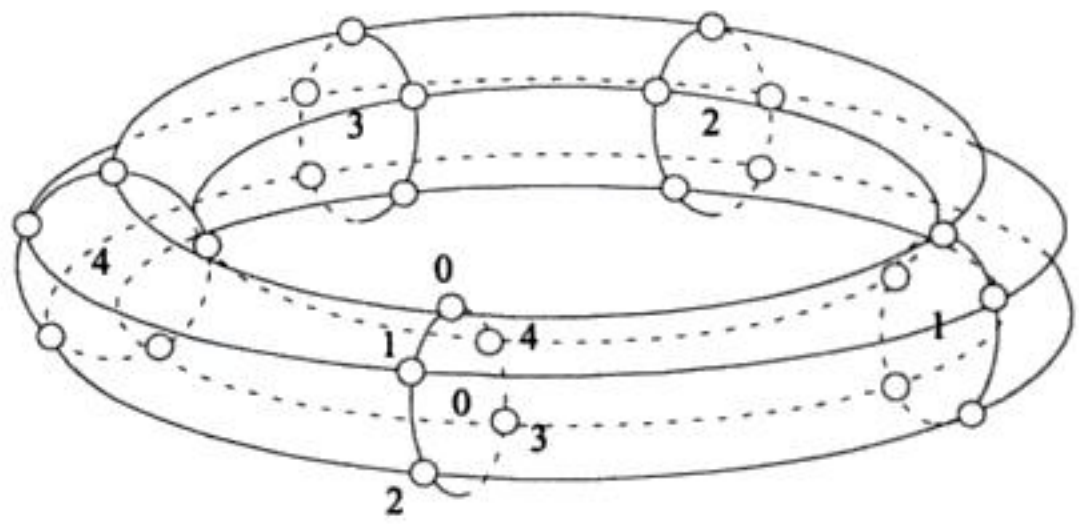
Este método está basado en que K=Z/5 es cuerpo. Es válido por tanto para Z/p siendo p un número primo.

Puede extenderse para órdenes potencia de primo ya que todos los cuerpos finitos deben tener un orden p^a con p primo.

La representación gráfica más interesante se obtiene dando a ambos ejes el carácter cíclico que tienen los elementos de K. Es decir, el valor siguiente a 4 es 4+1=0. Ello se consigue colocando el eje X sobre una circunferencia dividida en 5 partes lo que nos daría un cilindro.

Haciendo lo mismo con el eje Y vamos a parar a 25 puntos situados sobre la superficie de un toro más o menos como indica la figura.

Es curioso observar que la pendiente de una recta tiene un significado geométrico muy claro en la representación sobre el toro: indica el número de veces que la recta está arrollada sobre el círculo menor mientras se recorre una vuelta sobre el círculo mayor.



El dibujo es complicado de ver pero si se dispone de un modelo material es clarísimo.

Debe quedar patente que el método desarrollado genera cuadrados mágicos de orden primo, pero ni es el único método ni se afirma que no existan cuadrados mágicos para otros órdenes.

Hay muchos libros de matemáticas recreativas con métodos más rápidos para generar cuadrados mágicos de orden impar.

Copyrighted material

El interés del método expuesto estriba en la relación entre temas aparentemente dispares como el álgebra, la geometría, las estructuras finitas, los cuadrados mágicos y la representación sobre superficies topológicamente distintas del plano.

Copyrighted material

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

imposible ya que h < a, k < a, h – k < a, y b primo con a; luego no puede ser (h – k)b múltiplo de a.

LEMA 2

Si a < b son primos entre sí en Z, existen p, q $\in$ Z, tales que pa + qb = 1

En efecto, por lema 1 existe qb que da resto 1 al dividir por a:

$$qb = sa + 1 \Leftrightarrow pa + qb = 1,\ p = -s$$

TEOREMA DE BÉZOUT

Si m.c.d.(a,b) = d, existen p, q $\in$ Z, tales que: ap + bq = d.

Si a = da', b = db' será m.c.d.(a',b') = 1.

Por lema 2: pa' + qb´= 1 $\Rightarrow$ (pa' + qb')d = d $\Rightarrow$ pa + qb = d.

Caso particular de este teorema es el lema utilizado para demostrarlo.

TEOREMA DE EXISTENCIA

La ecuación lineal ax + by = c tiene solución entera si y sólo si

$$m.c.d.(a,b,c) = m.c.d.(a, b)$$

Es decir, si la ecuación simplificada tiene los coeficientes de las dos incógnitas, primos entre sí.

La ecuación ax + by + cz +...= k tiene solución entera si la tiene una de las ecuaciones con dos incógnitas, obtenida al suprimir los términos de todas las demás, que valdrán 0.

DEMOSTRACIÓN

Necesidad:

Supongamos la solución entera x = k, y = h, entonces c = ak + bh, y todo divisor de a y b lo es de c. En particular, tras simplificar, si

$$m.c.d.(a, b) = d \Rightarrow m.c.d.(a, b, c) = d = 1$$

Copyrighted material

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

EJEMPLO 4: $3x + 5y - 2z = 0$; $(x, y, z) = k\,(-5, 3, 0) + h\,(2, 0, 3)$.
Subespacio de dimensión $d = n\text{-}1 = 2$

EJEMPLO 5: $x + 5y - 2z + 7w = 0$
$(x, y, z, w) = k\,(-5, 3, 0, 0) + h\,(2, 0, 3, 0) + p\,(-7, 0, 0, 3)$; $d = 3$
$7x - 18y = 0$: $(x, y) = k\,(18, 7)$; $d = 1$

Al restringirnos a soluciones enteras hablaremos también, impropiamente, de subespacio, queriendo decir "parte del subespacio formada por vectores de coordenadas enteras". Debería decirse "módulo", que es la estructura similar a la de espacio vectorial, con anillo en vez de cuerpo. En realidad es subespacio con k, h cualesquiera. Aquí interesan sus valores enteros.

Solución general de una ecuación es el conjunto de todas sus soluciones particulares.

Consecuencia: La solución general de una ecuación lineal no homogénea se obtiene sumando a una cualquiera de sus soluciones particulares, la solución general de la homogénea asociada.

SOLUCIÓN DE ECUACIONES NO HOMOGÉNEAS

A) Método de congruencias (teorema de Bézout)

La solución particular se obtiene, para cualquiera número de incógnitas $n > 1$, eligiendo una parte con dos incógnitas, sea $ax + by = c$, que cumpla el criterio:

$$\text{mcd.}(a, b, c) = \text{mcd.}(a, b),$$

y que se resuelve aplicando el teorema de Bezout al par (a,b). Se da valor 0 a las demás incógnitas.

Aunque el estudio de múltiplos puede hacerse con hoja de cálculo o calculadora, por simple intuición también es rápido para números pequeños, si se practica un poco.

Para la solución general se añade la de su homogénea asociada obtenida en forma trivial.

EJEMPLO 6: $17x + 5y = 6$.

Tanteo para aplicar el lema 1 o el teorema de Bézout.

Se busca un múltiplo de 17 que difiera de otro de 5 en 6, en 1 o en cualquier otro divisor de 6.

Copyrighted material

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

x = 4. Soluciones naturales: (4,1,0), (4,0,3)

x = 3. Soluciones naturales: (3,2,1), (3,1,4), (3,0,7)

x = 2. Soluciones naturales: (2,3,2), (2,2,5), (2,1,8), (2,0,11)

x = 1. Soluciones naturales: (1,5,0), (1,4,3), (1,3,6), (1,2, 9), (1,1,12), (1,0,15)

x = 0. Soluciones naturales: (0,6,1), (0,5,4), (0,4,7), (0,3,10), (0,2,13), (0,1,16), (0,0,19)

SISTEMAS DE ECUACIONES LINEALES

Una ecuación lineal se transforma en otra equivalente por adición a sus dos miembros de una misma expresión lineal o una misma constante.

Un sistema lineal se transforma en otro equivalente eliminando una ecuación lineal que sea combinación lineal de las demás.

Un sistema lineal se transforma en otro equivalente sustituyendo una de las ecuaciones por su suma con una combinación lineal de las demás.

RESOLUCIÓN DE SISTEMAS LINEALES DIOFÁNTICOS

Utilizaremos el método de triangulación de Gauss en la modalidad que llamaremos mónica.

Polinomio mónico es aquel en que el coeficiente del término de mayor grado es la unidad.

El método de Gauss sistematiza el de reducción para sistemas lineales, transformándolos en otros equivalentes hasta conseguir uno que sea escalonado en el número de ceros iniciales.

La triangulación la llamaremos mónica si es 1 el primer coeficiente no nulo en cada ecuación, excepto la última, que puede no serlo.

El sistema, si es compatible, se resuelve comenzando por la última ecuación y siguiendo una a una por las anteriores, sustituyendo valores de incógnitas ya obtenidas, que serán enteras si lo han sido las de la última ecuación.

Copyrighted material

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

Operando desde atrás:

$$r_1 = \frac{5}{1};\ r_2 = 5 + \frac{1}{2} = \frac{11}{2};\ r_3 = \frac{115}{21};\ r_4 = \frac{241}{44};\ r_5 = \frac{2525}{461};\ r_6 = \frac{5291}{966};\ \ldots$$

$r_1 = 5$; $r_2 = 5'5$; $r_3 = 5'476...$; $r_4 = 5'47727...$; $r_5 = 5'477223...$; $r_6 = 5'477225...$; ...

Esas seis aproximaciones convergen alternativamente, y garantizan ya cinco decimales exactos:

$\sqrt{30} = 5'47722\ ...;\ 5 < 5'476 < 5'477223... < ... < 5'477225... < 5'47727 < 5'5$

ALGORITMO DE FRACCIONES CONTINUAS

Con la sucesión $a_1, a_2, a_3, ..., a_n, ...$ se construye otra, llamada de fracciones continuas:

$$R_1 = \frac{p_1}{q_1} = a_1 = \frac{a_1}{1}$$

$$R_2 = \frac{p_2}{q_2} = a_1 + \frac{1}{a_2} = \frac{a_1 a_2 + 1}{a_2} = \frac{(a_1, a_2)}{(a_2)}$$

$$R_3 = \frac{p_3}{q_3} = a_1 + \frac{1}{a_2 + \dfrac{1}{a_3}} = \frac{a_3(a_2 a_1 + 1) + a_1}{a_3 a_2 + 1} = \frac{(a_1, a_2, a_3)}{(a_2, a_3)} \quad (1)$$

.....

$$\frac{p_n}{p_n} = \frac{a_n p_{n-1} + p_{n-2}}{a_n q_{n-1} + q_{n-2}} = \frac{(a_1, a_2, ..., a_n)}{(a_2, a_3, ..., a_n)}$$

Son finitas o indefinidas según sea la sucesión (a_n) cuyos términos se llaman cocientes incompletos. Supondremos que son números entero positivos, excepto a_1, que puede ser 0.

Las fracciones continuas finitas definen el número racional que es su última fracción. Se unifica el lenguaje suponiendo que a la última fracción siguen otras infinitas idénticas a ella.

Si un grupo de cocientes incompletos se repite, la fracción continua se llama periódica.

Copyrighted material

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

b) Si $u_n = p(n)$ es de grado k, sus diferencias

$$\Delta u_n = u_{n+1} - u_n = p(n+1) - p(n) = g(n)$$

es de grado (k – 1), al desaparecer el término de mayor grado de p. Reiterando sale $\Delta^k u_n = cte$.

III. Una sucesión es progresión aritmética de orden k si y sólo si la suma de m términos es polinomio de grado k + 1.

Demostración: Análoga a la anterior desarrollando (10) en lugar de (9).

IV. Toda progresión aritmética de orden k es a su vez sucesión recurrente de orden (k + 1)

Demostración: De (7) con $\Delta^{k+1} u_1 = 0$ sale

$$u_{k+2} = \binom{k+1}{0} u_{k+2} = \binom{k+1}{1} u_{k+1} - \binom{k+1}{2} u_k + \ldots \pm \binom{k+1}{k+1} u_1$$

EJEMPLO 8

Obtención directa de la ecuación de recurrencia para una progresión aritmética de orden 3:

Sucesión: u_1,	u_2	$\ldots u_{n-1}$	u_n
Dif-1 $u_2 - u_1$	$u_3 - u_2$	$\ldots u_n - u_{n-1}$	$u_{n+1} - u_n$
Dif-2 $u_3 - 2u_2 + u_1$	$u_4 - 2u_3 + u_2$	$\ldots u_{n+1} - 2u_n + u_{n-1}$	$u_{n+2} - 2u_{n+1} + u_n$
Dif-3 $u_4 - 3u_3 + 3u_2 - u_1$		$\ldots u_{n+2} - 3u_{n+1} + 3u_n - u_{n-1}$	$u_{n+3} - 3u_{n+2} + 3u_{n+1} - u_n$
Dif-4 0	0	0	0

Al igualar las dos últimas sale la ecuación de recurrencia:

$$u_{n+3} = 4u_{n+2} - 6u_{n+1} + 4u_n - u_{n-1}$$

Otra forma de presentarla:

$$u_{n+5} = 4u_{n+4} - 6u_{n+3} + 4u_{n+2} - u_{n+1}$$

Se necesita además conocer los cuatro primeros términos: u_1, u_2, u_3, u_4

EJEMPLO 9: Obtención directa de ecuaciones de recurrencia

(a)

$$u_n = 3n + 2$$
$$u_{n+1} - u_n = 3(n+1) - 3n = 3$$
$$u_{n+2} - u_{n+1} = u_{n+1} - u_n$$
$$u_{n+2} = 2u_{n+1} - u_n$$

Copyrighted material

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

EJEMPLO 7: Sucesiones de Fibonacci.

Son las recurrentes de ecuación:

$$u_{n+2} = u_{n+1} + u_n (n \geq 1) \qquad (9)$$

En la estricta de Fibonacci es $u_1 = 1,\ u_2 = 1$; 1, 1, 2, 3, 5, 8, ...

El problema que originó la sucesión consiste en calcular la secuencia de producción en una granja de conejos, en número de parejas adultas, bajo los siguientes condiciones:

a) Por cada pareja de conejos adultos nace al mes una pareja de gazapos, macho y hembra

b) Los gazapos al cabo de un mes son ya adultos, con capacidad de reproducción.

Si u_n es el número de parejas adultas (por cada pareja inicial) en el n-ésimo mes; resultará:

$u_1 = 1$ (1 par de adultos y 0 gazapos)

$u_2 = 1$ (1 de adultos y 1 de gazapos)

$u_3 = 2$ (2 de adultos y 1 de gazapos)

$u_4 = 3$ (3 de adultos y 2 de gazapos)

$u_5 = 5$ (5 de adultos y 3 de gazapos)

... ...

$$u_{n+2} = u_{n+1} + u_n (n \geq 1) \quad (4)$$

EJEMPLO 8: Cociente creciente de polinomios.

Los coeficientes del cociente son sucesión recurrente de orden k, grado del denominador.

Si es $P(x) = A_0 + A_1 x + ... + A_1 x^1$; $Q(x) = B_0 + B_1 x + ... + B_k x^k$

$$\frac{P(x)}{Q(x)} = C(x) = D_0 + D_1 x + D_2 x^2 + ... + D_n x^n + ...$$

$$D_{n+k} = -\frac{B_1}{B_0} D_{n+k-1} - \frac{B_2}{B_0} D_{n+k-2} - ... - \frac{Bk}{B_0} D_n \ (n \geq 1 - k + 1) \qquad (10)$$

Demostración: Usando coeficientes indeterminados en C(x), al identificar C(x).Q(x) = P(x) se obtiene C(x)

Ejemplo:

$$\frac{1+x}{1-x^2} = 1 + x - x^2 - x^3 + x^4 + x^5 - ...$$

Copyrighted material

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

polinomios de grados conocidos, que sometidos a determinadas operaciones den un resultado ya previsto.

Ejemplo: Descomponer $x^2 + 3/4$ en diferencia de cuadrados de dos polinomios de grado dos.

$$x^2 + 3/4 = (x^2 + ax + b)^2 - (x^2 + cx + d)^2$$

que resulta ser:

$$x^2 + 3/4 = (x^2+1)^2 - (x^2+ 1/2)^2$$

Al identificar coeficientes en ambos miembros:

$$0 = 2(a - c)$$
$$1 = a^2 + 2b - c^2 - 2d$$
$$0 = 2ab - 2cd$$
$$3/4 = b^2 - d^2$$

Si no hubiéramos supuesto los trinomios mónicos, saldrían infinitas soluciones dependientes de un parámetro A, igual al primer coeficiente en uno de los trinomios, y al valor absoluto en el otro.

DIVISIÓN EN LÍNEA Y DIVISIÓN SINTÉTICA

Son dos formas de presentar un mismo procedimiento, que particulariza a la división de polinomios el método de los coeficientes indeterminados y generaliza el tan conocido algoritmo de Ruffini.

Nos limitaremos a dividir f(x) por g(x) con cociente q(x): $f = gq + r$, siendo #f=4 y #g=1 o #g=2

$$f(x)= a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 ;\ \ g(x) = (x - \alpha).$$

Se determina $q(x) = b_3x^3 + b_2x^2 + b_1x + b_0$, $r = k$, mediante las relaciones:

$$b_3 = a_4;\ b_2 = a_3 + \alpha b_3;\ b_1 = a_2 + \alpha b_2;\ b_0 = a_1 + \alpha b_1;\ r = a_0 + \alpha b_0$$

Los coeficientes se disponen en filas y columnas, en la forma sintética llamada algoritmo de Ruffini.

Lo mismo puede hacerse al dividir por un polinomio de segundo grado; incluso sin que sea mónico.

Copyrighted material

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

$$\frac{5x^3+2x^2-x+7}{(x^2+x+2)^2}=\frac{5x(x^2+x+2)-3(x^2+x+2)-8x+13}{(x^2+x+2)^2}=\frac{-8x+13}{(x^2+x+2)^2}+\frac{5x-3}{(x^2+x+2)}$$

PROPOSICIÓN

Regla de los signos de Descartes

Si σ es el número de ceros reales positivos de

$$p(x)=a_0+a_1x+a_2x^2+\ldots+a_nx^n \in R[x],$$

y τ el de cambios de signo de la sucesión de sus coeficientes, entonces $(\tau-\sigma)$ es número par y no negativo.

Análogamente el número σ de ceros negativos es el número τ de cambios de signo de $p(-x)$ o difiere de él en un entero par, ya que si $-\alpha$ es un cero negativo de $p(x)$, resulta α cero positivo de $p(-x)$.

DEMOSTRACIÓN: Sólo indicamos que se hace por inducción, sobre el número σ de ceros positivos de $p(x)$.

En el cómputo de cambios de signo, no cuentan los coeficientes nulos.

Corolarios:

1) Todo número real $a > 0$ tiene dos raíces n-ésimas reales si n es par

2) Todo número real $a < 0$ tiene una sola raíz n-ésima real si n es impar.

ESTIMACIÓN DE COTAS ENTRE LAS QUE OSCILAN LOS CEROS REALES DE UN POLINOMIO

Se fundamenta en la regla de Descartes y en la evidencia de que un polinomio con coeficientes positivos $p(x)$ no puede tener un cero positivo α, ya que $p(\alpha) > 0$. Hay variantes sugerentes de esta idea.

EJEMPLO 3

$p(x) = 3x^3 - 4x^2 - 17x + 6 = x^2(x-4) + x(2x^2-17) + 6 > 0$ si $x > 4$ y $x^2 > 8.5$

Por tanto no tiene raíces positivas mayores que 4.

$$-p(-x) = 3x^3 + 4x^2 - 17x - 6 = x(3x^2-17) + 4(x^2 - 3/2) > 0$$

y

$$p(-x) < 0 \text{ si } x > \sqrt{k}\ ,\ k = \text{máx}(17/3,\ 3/2)$$

No hay raíces negativas menores que $-\sqrt{k}$ .Todas las raíces están en [–2.6, 4].

Copyrighted material

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

II. El número de permutaciones que se pueden formar con m objetos, entre los cuales hay α que son iguales entre sí, otros β iguales, ..., λ iguales, es:

$$P_m^{\alpha,\beta,\ldots,\lambda} = \frac{m!}{\alpha!\beta!\ldots\lambda!} \quad (\alpha + \beta + \ldots + \lambda = m)$$

COMBINACIONES

DEFINICIÓN: Combinaciones de orden n de m objetos a_1, a_2, a_3, ..., a_n son los subconjuntos de n objetos que se pueden formar con ellos, de modo que dos de ellos difieran en algún objeto.

Las variaciones en cambio se diferencian por el orden o también por la naturaleza de los objetos.

FORMACIÓN: Se procede sucesivamente a partir de las de orden 1, luego las de orden 2, ... etc.

De cada combinación de orden (n – 1) se obtienen combinaciones distintas de orden n agregando a su derecha, cada uno de los elementos siguientes al último.

NÚMERO

$$V_{m,n} = C_{m,n} \cdot P_m \Rightarrow C_{m,n} = \frac{V_{m,n}}{P_m} = \frac{m(m-1)\ldots(m-n+1)}{n!} = \frac{m!}{n!(m-n)!} = \binom{m}{n}$$

Si en una combinación de orden n hacemos permutaciones se obtienen las variaciones de orden n.

Se admite que 0! = 1, cuando el orden sea n = m.

Se anticipa aquí ya el símbolo de los números combinatorios.

COMBINACIONES CON REPETICIÓN

DEFINICIÓN: Combinaciones con repetición, de orden n, de m objetos, son los "subconjuntos" de n de esos objetos, repetidos o no, considerando iguales las que tienen los mismos objetos repetidos las mismas veces. Con m objetos se pueden formar combinaciones con repetición de un orden n > m.

FORMACIÓN: Se comienza por las de orden 1, luego las de orden 2, ... etc.; siguiendo este criterio.

Copyrighted material

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

TRIÁNGULO DE TARTAGLIA

m = 1								1				1									
m = 2							1			2			1								
m = 3						1			3			3			1						
m = 4					1			4			6			4			1				
m = 5				1			5			10			10			5			1		
m = 6			1			6			15			20			15			6			1

- Las filas son series completas de números combinatorios de numerador m: 1, 2, 3, 4, ...
- Los elementos de cada diagonal (desde el segundo) son suma de los de la diagonal anterior.
- Los elementos de la segunda diagonal (sumas de la primera, 1,1,1,...) son los números naturales.
- Los de la tercera se llaman números triangulares y cada uno resulta del anterior al añadirle el número ordinal del nuevo término.

$$\binom{1}{1}+\binom{2}{1}+\binom{3}{1}+\ldots+\binom{n}{1}=\binom{n+1}{2}\quad 1+2+3+\ldots+n=\frac{(n+1)n}{2}$$

Se llaman triangulares porque representan el número de puntos de una red triangular que tenga n puntos en la base, puesto que resultan por adición de los números naturales sucesivos.

- Los de la cuarta diagonal por la izquierda se llaman triángulo-piramidales y se obtienen por adición de los triángulos sucesivos. El de orden n viene dado por la expresión:

$$\binom{2}{2}+\binom{3}{2}+\binom{4}{2}+\binom{5}{2}+\ldots+\binom{n+1}{2}=\binom{n+2}{3}$$

$$1+3+6+10+15+\ldots+\frac{(n+1)n}{2}=\frac{(n+2)(n+1)n}{6}$$

Representa el número de puntos de una red piramidal con base una red triangular de orden n

- Si hacemos a = 2, b = 1 la segunda diagonal son los impares 1, 3, 5, 7, ... Los de la tercera se llaman números cuadrangulares y resultan por adición de los impares. El de orden n es:

Copyrighted material

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

Claramente hay 10 oros, 4 ases y 1 as de oros:

$$10 + 4 - 1 = 13$$

Daremos dos aplicaciones importantes:

a) Cuando A y B no tienen parte común, entonces la fórmula queda:

$$c(A \cup B) = c(A) + c(B)$$

Ejemplo: De cuántas maneras podemos extraer una carta de una baraja española de 40 cartas imponiendo que sea oros o bastos.

Ahora tenemos 10 oros, 10 bastos y ninguna carta es a la vez oros y bastos, por tanto:

$$10 + 10 = 20$$

b) Si A y B son disjuntos y es fácil calcular $c(A \cup B)$ y $c(A)$ se despeja $c(B) = c(A \cup B) - c(A)$

Ejemplo: Tiramos 6 monedas al aire, denotaremos con "+" el resultado "sale cara" y con "–" el resultado "sale cruz". ¿De cuántas maneras puedo obtener el resultado "al menos una cara"?

El resultado de una tirada es una lista de 6 signos elegidos entre "+" y "–".

Si intentamos contar directamente el número de resultados que tienen al menos una cara, al instante se aprecia su complejidad, puede haber una cara que esté en 6 posiciones o bien dos caras en las posiciones 1-2, o 1-3,....

Pensamos entonces en lo contrario de "alguna cara" que es "ninguna cara", cosa que se produce de una sola manera (-,-,-,-,-,-).

Los conjuntos asociados a los sucesos "alguna cara" (A) y "ninguna cara" (B) son disjuntos y su unión es el conjunto de todos los posibles resultados ambos fáciles de contar, por tanto:

$$c(A) = c(A \cup B) - c(B) = 2^6 - 1 = 63$$

La complejidad del recuento directo queda justificada por el resultado, son "casi todos".

LA REGLA MULTIPLICATIVA

Si tenemos dos conjuntos finitos A y B de cardinales n y m respectivamente y nos preguntamos por el número de parejas ordenadas con el primer elemento de A y el segundo de B estamos buscando el cardinal del conjunto A x B (producto cartesiano).

Copyrighted material

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

3.

$$(p-a)(p-b)(p-c) \le \frac{abc}{8}$$

siendo válida la igualdad si y sólo si el triángulo es equilátero.

En efecto, trivialmente tenemos:

$$\sqrt{a^2-(b-c)^2} \le a \Leftrightarrow \sqrt{(a+b-c)(a-b+c)} \le a$$

y sus análogas cambiando cíclicamente a, b, c. Escribiendo las tres desigualdades y multiplicándolas queda:

$$\left.\begin{array}{l}\sqrt{(a+b-c)(a-b+c)} \le a\\ \sqrt{(b+a-c)(b-a+c)} \le b\\ \sqrt{(c-a+b)(c+a-b)} \le c\end{array}\right\} \Rightarrow \sqrt{(a+b-c)^2(a-b+c)^2(-a+b+c)^2} \le abc\,.$$

Todos los paréntesis son positivos y además,

$$(a+b-c)=(a+b+c-2c)=2p-2c=2(p-c)$$

y sus análogos. Extrayendo la raíz positiva y sustituyendo queda:

$$8(p-c)(p-b)(p-a) \le abc \Leftrightarrow (p-a)(p-b)(p-c) \le \frac{abc}{8}$$

El signo igual es válido cuando lo sea en las desigualdades iniciales lo que exige $b = c = a$.

4.

$$R \ge 2r$$

En el tema 16 hay una demostración en términos puramente geométricos. Ahora podemos demostrarlo como consecuencia de la desigualdad anterior y de dos propiedades elementales:

a) $S = pr$ que expresa el hecho de que el área de un triángulo es suma de las áreas de los tres triángulos obtenidos uniendo el incentro con los tres vértices.

b) $abc = 4Rrp$. En efecto, $2S = bc\,\mathrm{sen}A$ y por el teorema de los senos

$$a = 2R\,\mathrm{sen}A \Rightarrow abc = 2bcR\,\mathrm{sen}A = 4RS = 4Rrp.$$

Para demostrar $R \ge 2r$, por la desigualdad 3, tenemos:

$$8(p-a)(p-b)(p-c) \le abc$$

por otra parte, la fórmula de Heron (ver tema 16) dice: $S = \sqrt{p(p-a)(p-b)(p-c)}$, multiplicando la desigualdad anterior por p queda:

Copyrighted material

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

Resumiendo:

$$\sqrt[n]{z} = \sqrt[n]{r}\left(\cos\frac{\varphi + 2k\pi}{n} + i\,\text{sen}\frac{\varphi + 2k\pi}{n}\right); k = 0, 1, ..., n-1$$

Obviamente la representación geométrica los afijos correspondientes a las raíces n-ésimas de un complejo dado z son los vértices de un polígono regular de n lados centrado en el origen.

Haciendo en la fórmula anterior $r = 1$ y $\varphi = 0$, obtenemos los n complejos u_k dados por:

$$\text{siendo } \varphi_k = \frac{2k\pi}{n}\ ;\ k = 0,\ 1, ..., n - 1$$

que son las n raíces n-ésimas de la unidad. Sobre el plano complejo se representan en los vértices de un n-ágono regular inscrito en la circunferencia unidad.

La estructura del conjunto $U_n = \{\ u_k \mid (u_k)^n = 1\ \}$ de las raíces n-ésimas de la unidad es especialmente interesante debido a la siguiente propiedad:

Si multiplicamos una raíz n-ésima cualquiera z' de z por una raíz n-ésima de la unidad se obtiene otra raíz n-ésima de z.

En efecto, si $(z')^n = z$; entonces $(z'u_k)^n = (z')^n\,(u_k)^n = (z')^n\ 1 = z$.

Por tanto, al multiplicar una raíz cualquiera z' por todos los elementos de U_n se obtienen todas las raíces n-ésimas de z.

Al multiplicar elementos de U_n el resultado pertenece a U_n. En particular cualquier potencia de un elemento de U_n también pertenece a U_n ya que $((u_k)^p)^n = ((u_k)^n)^p = 1^p = 1$.

RAÍCES PRIMITIVAS DE LA UNIDAD. POLINOMIOS CICLOTÓMICOS

Sea u_k un elemento de U_n, consideremos el conjunto de las n primeras potencias de u_k:

$$Uk = \left\{u_k, u_k^2, u_k^3, ..., u_k^n\right\}$$

Para aquellos valores de k para los que $U_k = U_n$ la correspondiente raíz u_k se llama raíz primitiva de la unidad.

EJERCICIO 5: Para un n dado probar que u_k es raíz primitiva si y sólo si k y n son primos entre sí.

Si n es primo, todas las raíces distintas de 1 son primitivas y hay $n - 1$ raíces primitivas.

Copyrighted material

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

b) $\operatorname{sen} x + \operatorname{sen} 2x + ... + \operatorname{sen} nx = \dfrac{\operatorname{sen}\dfrac{(n+1)x}{2}}{\operatorname{sen}\dfrac{x}{2}} \operatorname{sen}\dfrac{nx}{2}$

Solución:

Pongamos:

$A = 1 + \cos x + \cos 2x + \cos 3x + ... + \cos nx; \quad B = \operatorname{sen} x + \operatorname{sen} 2x + \operatorname{sen} 3x + ... + \operatorname{sen} nx$

suponiendo $x \neq 2k\pi$ puede sumarse como una progresión geométrica en la forma:

$$A + Bi = 1 + e^{ix} + e^{i2x} + e^{i3x} + ...e^{inx} = \frac{e^{i(n+1)x} - 1}{e^{ix} - 1} = \frac{\cos(n+1)x + i\operatorname{sen}(n+1)x - 1}{\cos x + i\operatorname{sen} x - 1}$$

usando las identidades $\cos\alpha = \cos^2\dfrac{\alpha}{2} - \operatorname{sen}^2\dfrac{\alpha}{2}$; $\operatorname{sen}\alpha = 2\operatorname{sen}\dfrac{\alpha}{2}\cos\dfrac{\alpha}{2}$ y operando, queda:

$$A + Bi = \frac{-2\operatorname{sen}^2\dfrac{(n+1)x}{2} + 2i\operatorname{sen}\dfrac{(n+1)x}{2}\cos\dfrac{(n+1)x}{2}}{-2\operatorname{sen}^2\dfrac{x}{2} + 2i\operatorname{sen}\dfrac{x}{2}\cos\dfrac{x}{2}} = \frac{\operatorname{sen}\dfrac{(n+1)x}{2}}{\operatorname{sen}\dfrac{x}{2}} \cdot \frac{\cos\dfrac{(n+1)x}{2} + i\operatorname{sen}\dfrac{(n+1)x}{2}}{\cos\dfrac{x}{2} + i\operatorname{sen}\dfrac{x}{2}}$$

Multiplicando por el conjugado del último denominador, resulta:

$$A + Bi = \frac{\operatorname{sen}\dfrac{(n+1)x}{2}}{\operatorname{sen}\dfrac{x}{2}} \frac{\left(\cos\dfrac{(n+1)x}{2} + i\operatorname{sen}\dfrac{(n+1)x}{2}\right)\left(\cos\dfrac{x}{2} - i\operatorname{sen}\dfrac{x}{2}\right)}{\cos^2\dfrac{x}{2} + \operatorname{sen}^2\dfrac{x}{2}} = \frac{\operatorname{sen}\dfrac{(n+1)x}{2}}{\operatorname{sen}\dfrac{x}{2}} e^{\frac{(n+1)x}{2} - \frac{x}{2}} =$$

$$= \frac{\operatorname{sen}\dfrac{(n+1)x}{2}}{\operatorname{sen}\dfrac{x}{2}} e^{\frac{nx}{2}} = \frac{\operatorname{sen}\dfrac{(n+1)x}{2}}{\operatorname{sen}\dfrac{x}{2}}\left(\cos\frac{nx}{2} + i\operatorname{sen}\frac{nx}{2}\right)$$

Igualando las partes real e imaginaria se obtiene el resultado.

COMPLEJOS Y GEOMETRÍA

En lo que sigue vamos a interpretar las operaciones definidas en los complejos desde el punto de vista de su representación gráfica en el llamado plano complejo (o de Argand).

Copyrighted material

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

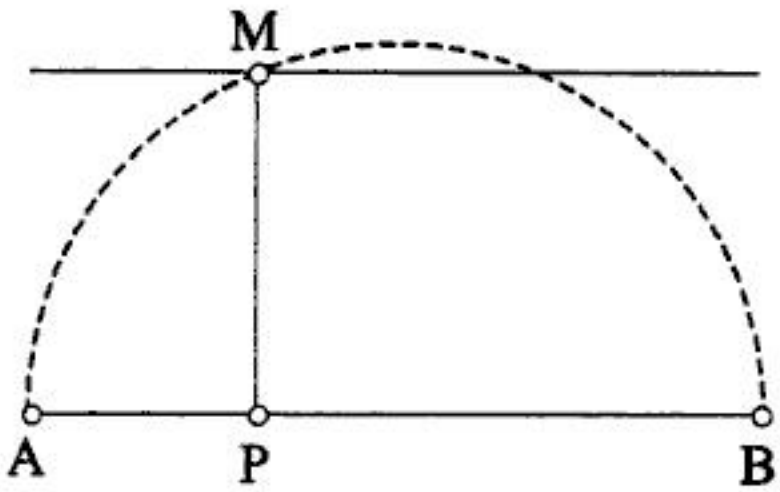
You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



Con $s > 0$ y $p > 0$ en todos los casos.

Denotemos a las raíces por a y b.

Caso 1: Las dos raíces son del mismo signo siendo

$$p = |a \cdot b| \text{ y } s = |a + b| .$$

El signo de las raíces es el contrario al de s en [1].

Luego basta saber hallar dos números positivos |a| y |b| conociendo su suma s y su producto p.

Para ello se siguen los siguientes pasos:

1. Se traza una semicircunferencia de diámetro s.
2. Se traza una paralela al diámetro AB a una distancia $\sqrt{p}$.
3. Por una de las dos intersecciones (M en el dibujo) se traza la perpendicular a AB por M.

El punto P, pie de esta perpendicular divide al segmento en dos partes que son |a| y |b|. Los signos se toman según lo expuesto antes.

La justificación es evidente por el teorema de la altura.

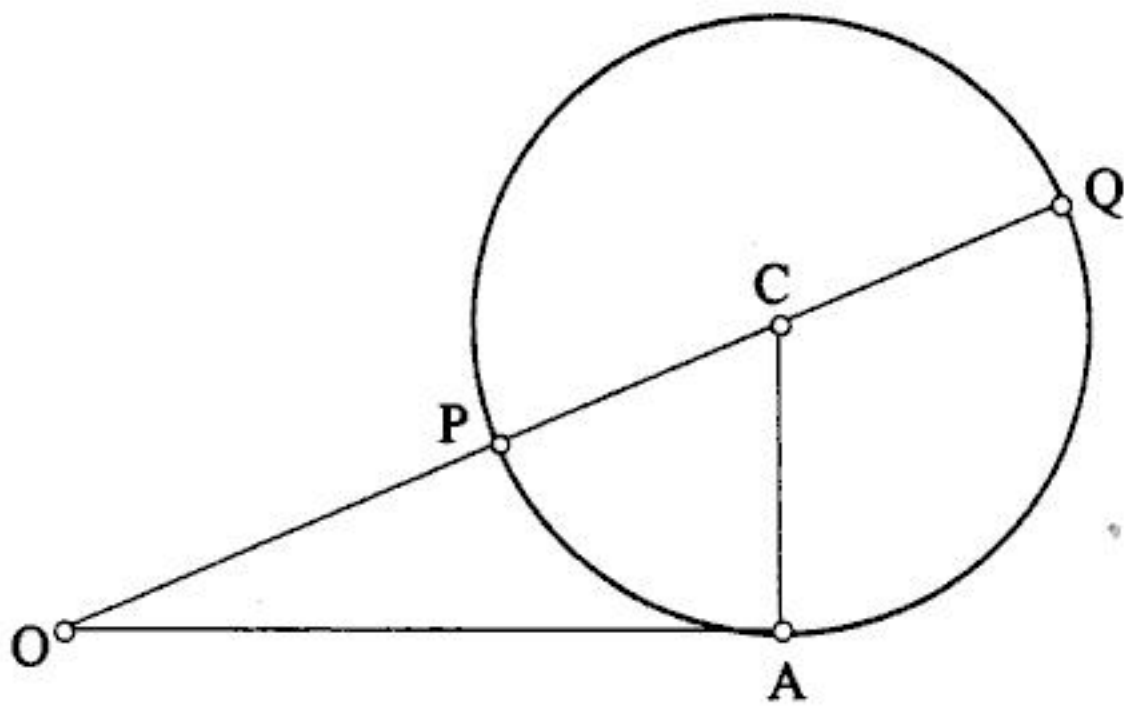
Notemos que el paso 2 requiere una de las contrucciones anteriores.

Caso 2: Las dos raíces tienen signos contrarios, con lo que $|a \cdot b| = p$ y $a - b = d$.

El problema se reduce a hallar dos números conociendo su producto p y su diferencia d.

El signo de d en [2] se adjudica a la raíz de mayor valor absoluto, la otra tendrá el contrario.

La construcción está indicada en la figura siguiente.



Copyrighted material

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

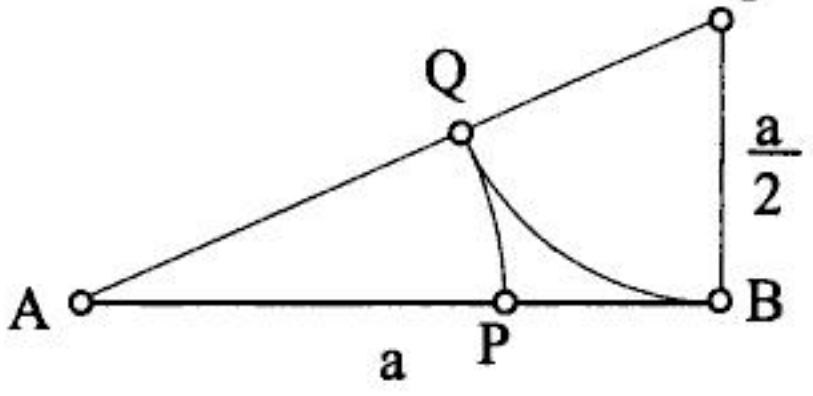
You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

$$r = \frac{L}{x} = \frac{1+\sqrt{5}}{2}$$

Llamada proporción áurea, esta relación aparece en multitud de situaciones.

Para construir el segmento áureo de un segmento dado de longitud a basta construir el valor de r hallado, para ello:



1. Se construye un triángulo rectángulo cuyo cateto mayor es el segmento AB de longitud a dado. El cateto menor tiene longitud mitad.
2. Con centro en C se lleva el cateto menor sobre la hipotenusa obteniendo el punto Q.
3. Con centro en A se abate AQ sobre AB determinando la solución AP.

La justificación del procedimiento es sencilla: basta calcular la longitud AP en función de a. Se deja como ejercicio.

Copyrighted material

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

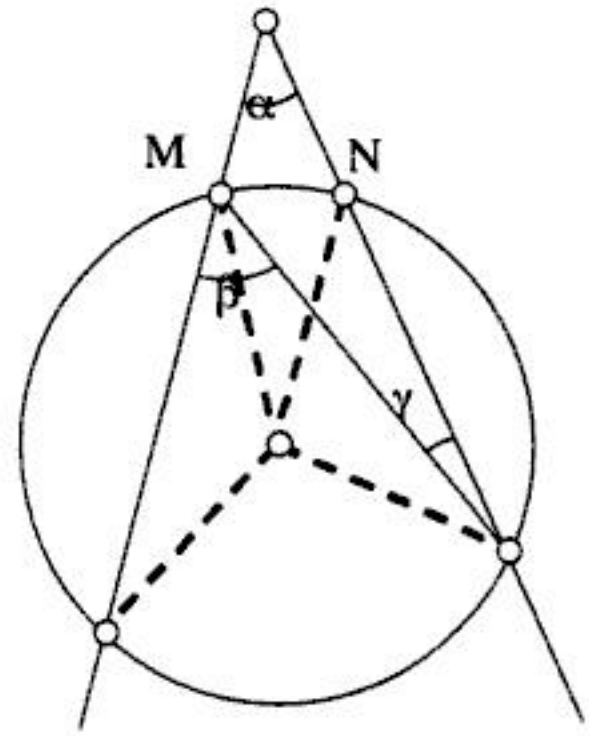
You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

ÁNGULO EXTERIOR

Es el que tiene el vértice fuera de la circunferencia y los lados son dos secantes. En este caso la idea de ángulo central se traduce en dos, ambos con vértice en el centro y abarcando los dos arcos interiores del ángulo dado.

TEOREMA 3

El ángulo exterior vale la semidiferencia de los dos arcos centrales.



Demostración: En la figura de la derecha se han trazado segmentos auxiliares de trazo fino y son evidentes las siguientes igualdades:

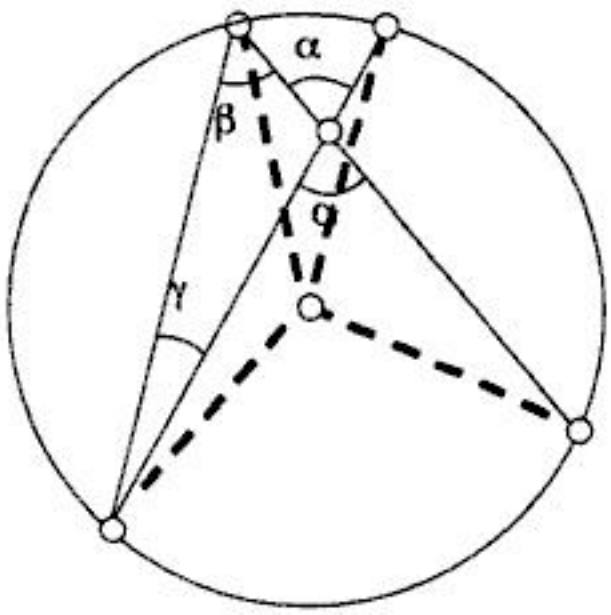
$$\beta = \alpha + \gamma \Rightarrow \alpha = \beta - \gamma = \frac{\angle COB - \angle MON}{2}$$

y el teorema queda demostrado.

Ejercicio: Demostrar que el resultado es igualmente válido si uno o los dos lados son tangentes a la circunferencia.

ÁNGULO INTERIOR

Es el que tiene el vértice dentro de la circunferencia y los lados son dos secantes. De nuevo hay dos ángulos centrales, ambos con vértice en el centro y abarcando los dos arcos interiores del ángulo dado.



TEOREMA 4

El ángulo interior vale la semisuma de los dos arcos centrales.

Demostración: Basta observar la figura y usar la propiedad del ángulo exterior de un triángulo.

$$\alpha = \beta + \gamma = \frac{\angle COB + \angle MON}{2}$$

APLICACIONES

Arco capaz de un ángulo dado sobre un segmento.

Copyrighted material

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

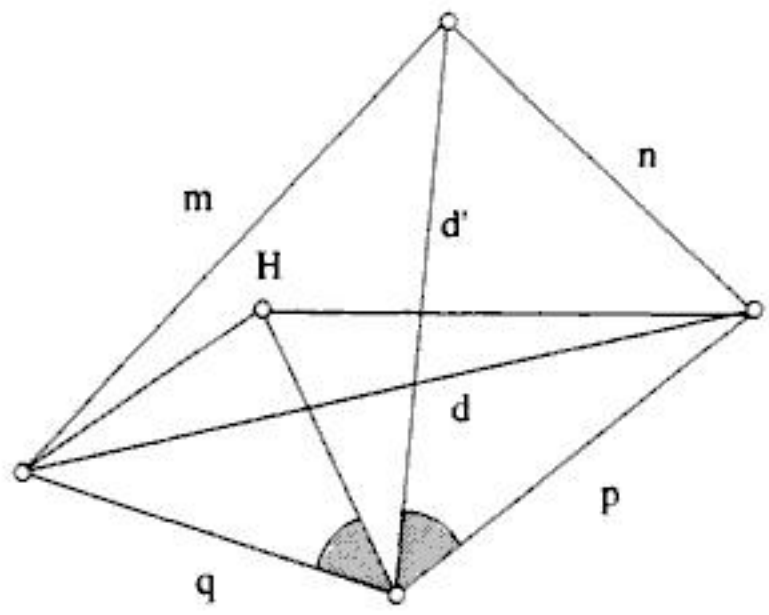
You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

Para n = 3, 4, 6, tanto la construcción como la demostración de las fórmulas de la tabla anterior son sencillas y se dejan como ejercicio.

Para demostrar los dos casos restantes necesitamos algún resultado previo.

TEOREMA DE TOLOMEO

La condición necesaria y suficiente para que un cuadrilátero sea convexo e inscriptible es que el producto de sus diagonales sea igual a la suma de los productos de los lados opuestos.



Demostración: Consideremos el cuadrilátero de la figura de vértices ABCD, lados m,n,p,q y diagonales d y d'.

Construimos un triángulo AHB semejante al DCB de forma que el lado q se corresponda con d' y los ángulos con vértice en B marcados en la figura sean iguales. Por la semejanza se cumple:

$$\frac{\overline{BH}}{p} = \frac{q}{d'} = \frac{\overline{AH}}{n} \Leftrightarrow q \cdot n = \overline{AH} \cdot d' \quad [1]$$

La primera de las igualdades de la proporción junto a la igualdad de los ángulos marcados establece que los triángulos HBC y ABD tambien sean semejantes (un ángulo igual y proporcionales los lados que lo forman), por tanto:

$$\frac{\overline{HC}}{m} = \frac{p}{d'} \Leftrightarrow p \cdot m = \overline{HC} \cdot d' \quad [2]$$

Y sumando las igualdades [1] y [2] queda:

$$q \cdot n + p \cdot m = \overline{AH} \cdot d' + \overline{HC} \cdot d' \geq \overline{AC} \cdot d' = d \cdot d'$$

Desigualdad válida para cualquier cuadrilátero.

El teorema estará demostrado cuando veamos la condición para que valga la igualdad:

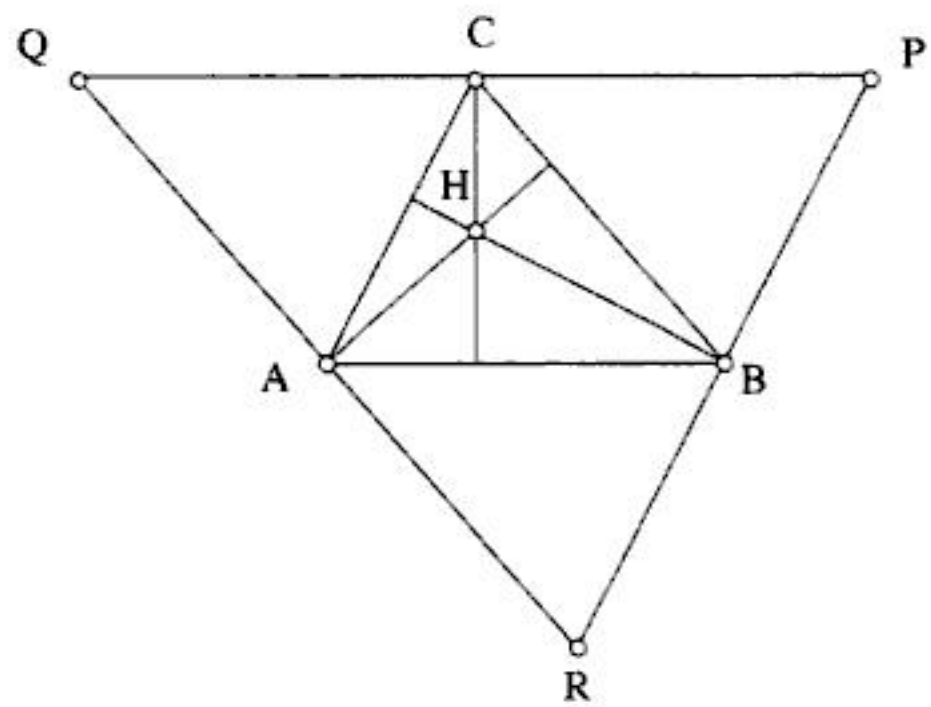
Copyrighted material

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

ALTURAS. ORTOCENTRO



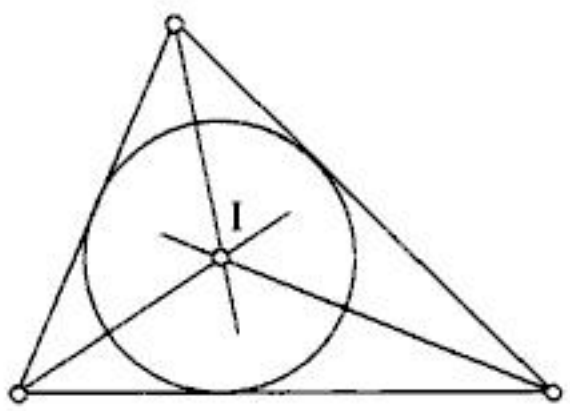
Al trazar las tres alturas del triángulo ABC se observa que se cortan en un mismo punto H llamado ortocentro como ahora demostraremos:

En efecto, basta trazar una paralela por cada vértice al lado opuesto de longitud doble. Con ellas se determina un triángulo PQR cuyas mediatrices son las alturas del triángulo dado. La concurrencia de las tres alturas queda reducida al caso anterior.

BISECTRICES: INCENTRO

Si llamamos I al punto de corte de bisectrices que parten de A y B, I equidista de los tres lados, luego la tercera bisectriz ha de pasar por el mismo punto I. Por tanto queda demostrado que las tres bisectrices son concurrentes.

Al punto I se le denomina incentro y es el centro de una circunferencia inscrita en el triángulo y tangente a sus tres lados.



También queda probado que existe una única circunferencia interior tangente a los tres lados de un triángulo.

El incentro es el único punto interior al triángulo que equidista de los tres lados. Si suprimimos la condición de ser interior, aparecen otros puntos del plano con la misma propiedad de equidistar de los tres lados considerados como rectas.

EXINCENTROS

Para localizar los puntos restantes hay que manejar las bisectrices exteriores, es decir prolongar los lados del triángulo y tener en cuenta que el conjunto de puntos que

Copyrighted material

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

De las fórmulas [1] y [2] extraeremos dos consecuencias:

En primer lugar si despejamos de [1] la mediana tendremos la longitud de una mediana en función de los lados:

$$\overline{CM}^2 = \frac{a^2 + b^2}{2} - \frac{c^2}{4}$$

Y, en segundo, si hacemos A y B fijos y los segundos miembros constantes obtenemos los lugares geométricos de los puntos cuya suma o diferencia de cuadrados a dos puntos fijos es constante:

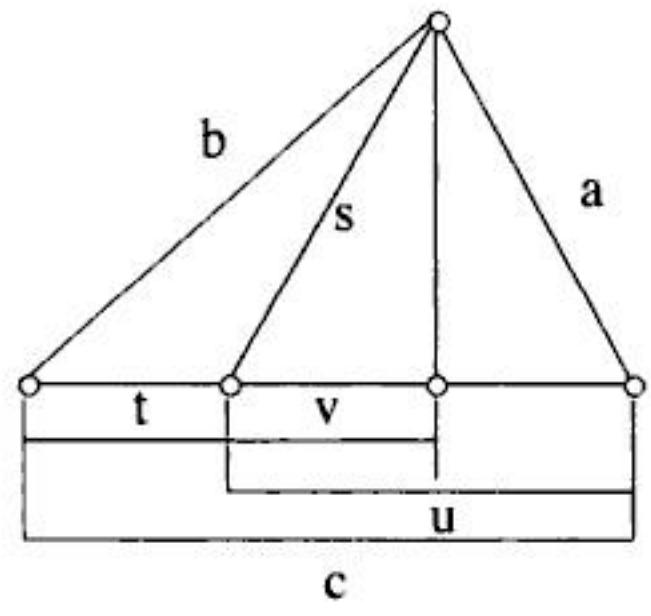
Para que la suma de cuadrados sea constante ha de serlo el segundo miembro de [1] siendo C variable con lo que tiene que ser la mediana de longitud constante y el lugar pedido es una circunferencia de centro el punto medio entre A y B y radio la mediana.

Para que la diferencia de cuadrados sea constante ha de serlo el segundo miembro de [2] o lo que es lo mismo, el segmento MH ha de tener longitud fija y C debe moverse en una recta perpendicular a AB que es el lugar geométrico buscado.

TEOREMA DE STEWART

Es una generalización de la fórmula [1] anterior cuando CM no es una mediana.

Aplicando el teorema anterior a los lados b y a en los triángulos MAC y MCB respectivamente:



$$b^2 = s^2 + t^2 + 2tv$$

$$a^2 = s^2 + u^2 - 2uv$$

Sólo queda eliminar v, para ello despejamos v de ambas ecuaciones, igualamos y operamos:

$$s^2(u + t) + ut(u + t) = b^2u + a^2t$$

y sustituyendo $u + t = c$ queda finalmente el teorema de Stewart:

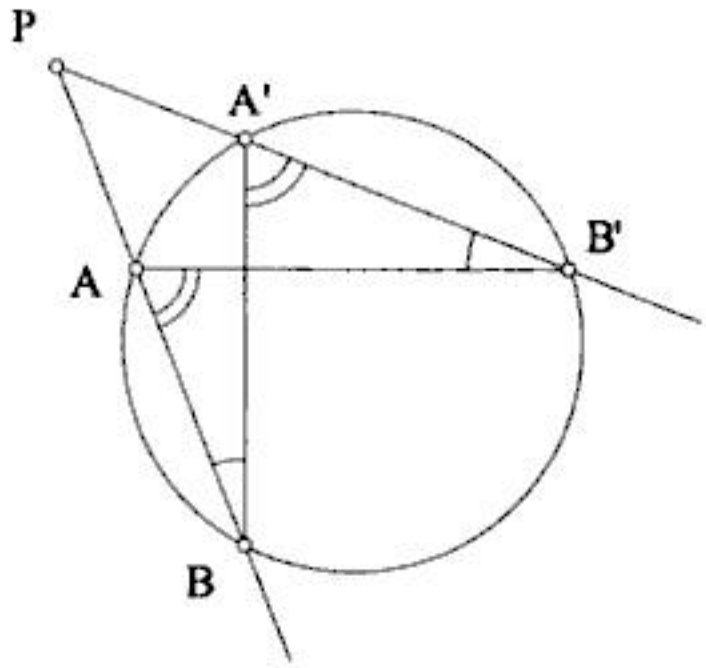
$$c(s^2 + ut) = b^2u + a^2t$$

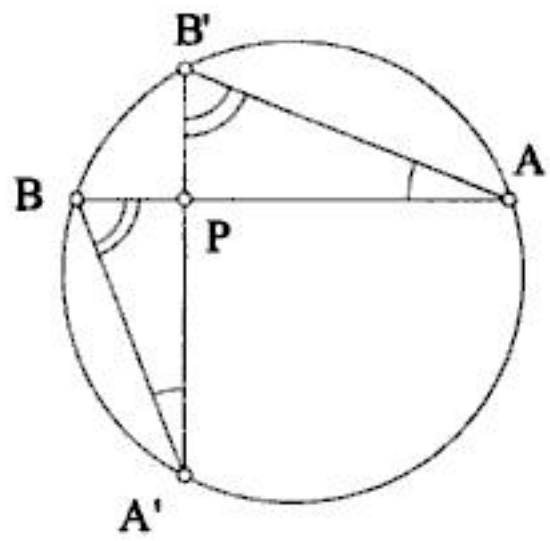
Copyrighted material

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



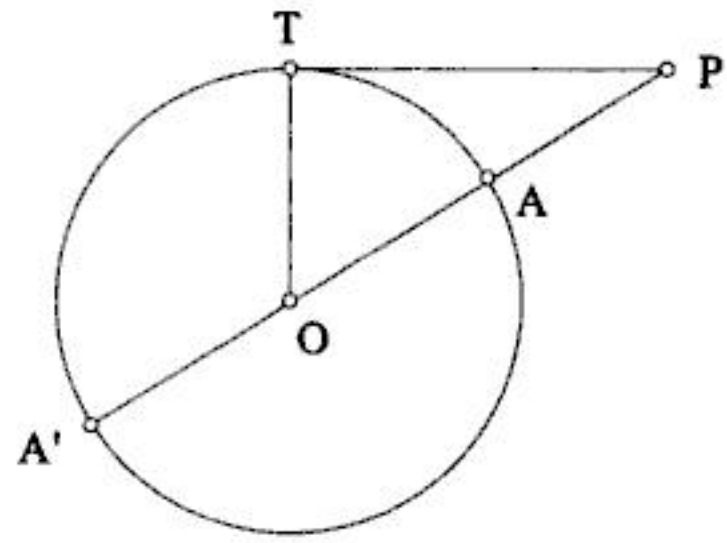


Ahora tiene sentido definir potencia de un punto respecto de una circunferencia como el valor de la constante de la demostración anterior, es decir como el producto PA·PA' para cualquier secante que pase por P.

En particular hay dos secantes especiales: la que pasa por el centro y la que es tangente.

Con ellas, y llamando d = PO, y r = OT obtenemos para la potencia las expresiones:

$$\overline{PA}\cdot\overline{PA'} = (d-r)\cdot(d+r) = d^2 - r^2 = \overline{PT}^2$$



La primera pone de manifiesto la dependencia de la potencia como función del radio y la distancia, además de darnos el signo. Los puntos exteriores a C tienen potencia positiva, los interiores negativa y los que están en C nula.

La segunda expresión sólo tiene sentido si P es exterior y resulta muy útil para multitud de problemas y construcciones geométricas.

EJE RADICAL DE DOS CIRCUNFERENCIAS

Dadas dos circunferencias C y C', de centros O, O' y radios r, r', nos proponemos buscar todos los puntos P del plano que tengan la misma potencia respecto de las dos circunferencias.

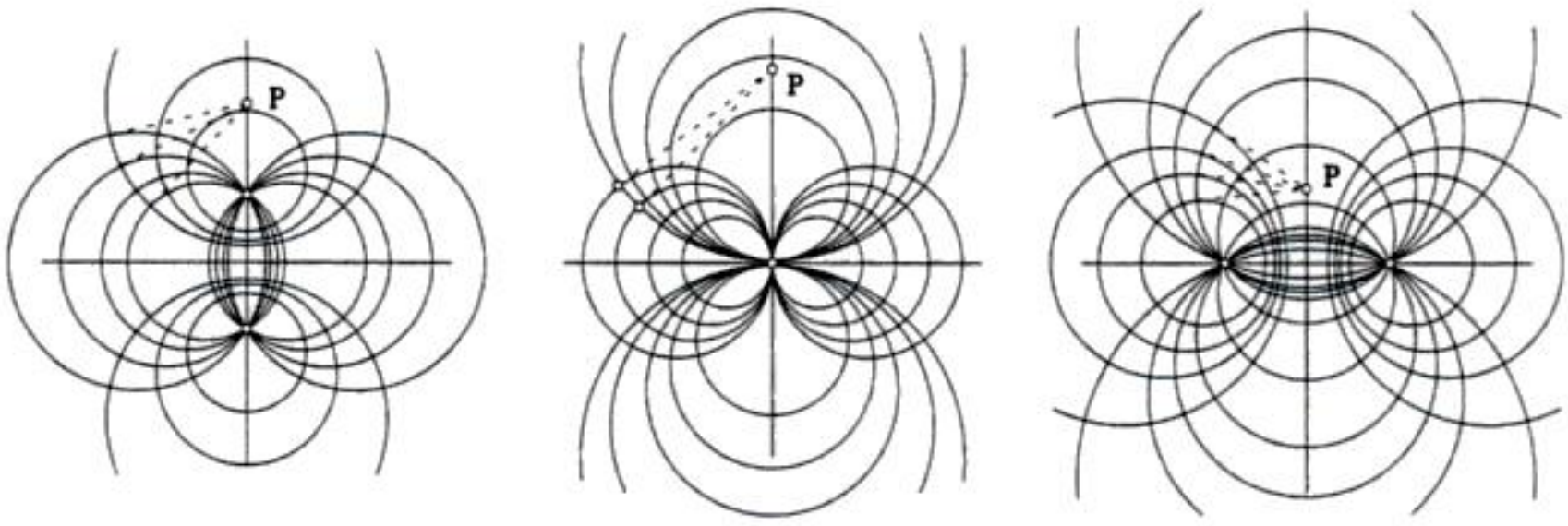
En virtud de la expresión encontrada antes y llamando d y d' a las distancias de P a O y O' respectivamente tendremos que P verifica la condición si y sólo si:

Copyrighted material

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



las tangentes a las mismas, el segmento que une P con el punto de tangencia tendrá longitud constante, dicho de otro modo, la circunferencia con centro en P y radio el segmento dicho será ortogonal a todas las circunferencias del haz.

Recíprocamente, toda circunferencia del haz es ortogonal a cualquier circunferencia con centro en el eje radical del haz dado y construida del modo antes descrito y por tanto su centro tiene la misma potencia respecto de todas ellas luego está en el eje radical de ellas.

Resumiendo: Si llamábamos H a un haz de circunferencias y H' al conjunto de todas las circunferencias ortogonales a las H, se cumple:

1. Toda circunferencia de H' tiene su centro en el eje radical de H.
2. Toda circunferencia de H es ortogonal a todas las de H'.
3. H' forma un haz cuyo eje radical es la recta que contiene a los centros de las circunferencias de H.

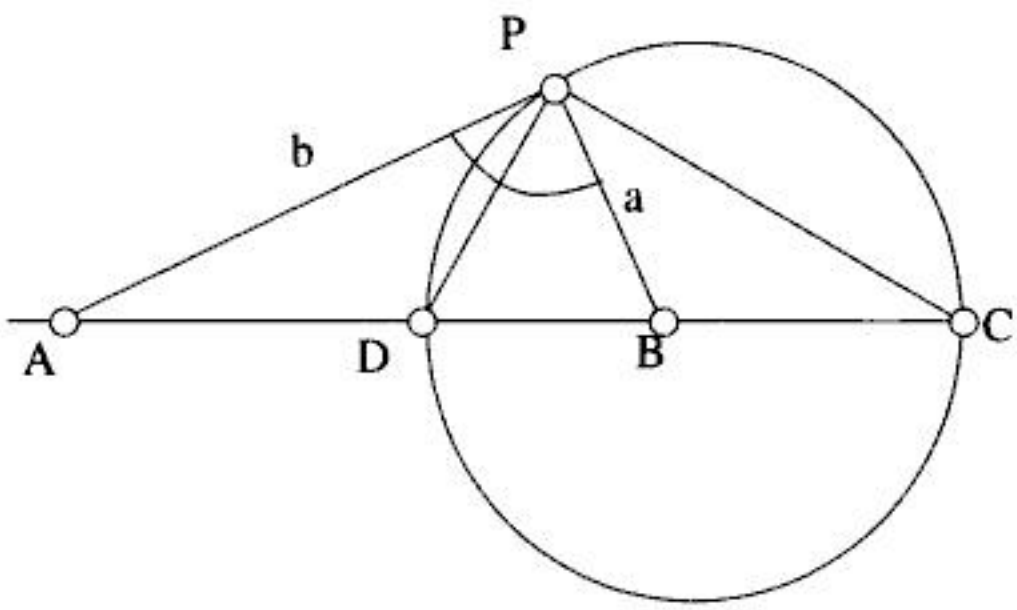
A estos haces los llamaremos haces ortogonales. Su disposición geométrica, según se indica en las figuras, empareja los tipos de forma cruzada: Si H es del tipo 1, H' es del 3. Si H es del tipo 2 H' también lo es y si H es del tipo 3 entonces H' es del tipo 1.

Copyrighted material

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



Para ello supongamos que A y B son fijos y dejamos P variable de modo que:

$$\frac{\overline{PB}}{\overline{PA}} = \frac{a}{b} = K$$

Pero de [1] y [2] tenemos:

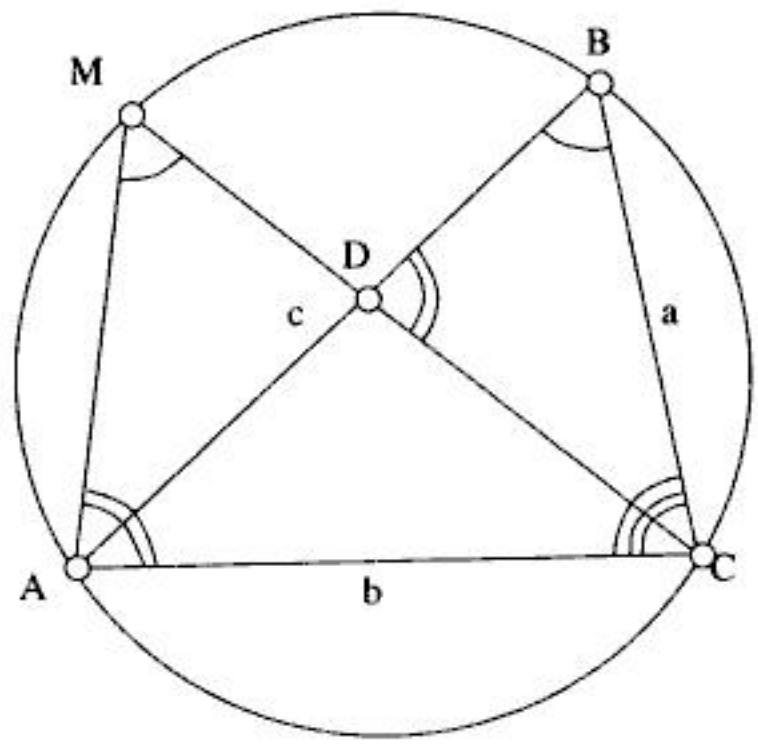
$$\frac{\overline{BC}}{\overline{AC}} = \frac{\overline{DB}}{\overline{AD}} = \frac{a}{b} = K$$

Luego C y D han de ser fijos por ser los únicos puntos de la recta AB cuya razón de distancias a A y B es constante.

Si los pies de las bisectrices han de ser fijos y éstas son constantemente perpendiculares, P ha de estar en el arco capaz de 90º sobre DC, es decir, el lugar de P es la circunferencia de la figura de diámetro DC.

Implícitamente hemos supuesto K distinto de 1. Si fuese K = 1 la igualdad [2] no es cierta pero para K = 1 el lugar pedido es trivialmente la mediatriz del segmento AB.

CÁLCULO DE LAS BISECTRICES



En la figura de la derecha se ha trazado la bisectriz interior que parte de C en el triángulo ABC. Además se ha trazado el círculo circunscrito y el punto M de intersección de éste con la prolongación de la bisectriz. Queremos hallar la longitud del segmento CD en función de los lados a, b, c.

Los triángulos MAC y DBC son semejantes por tener los ángulos iguales, (Los marcados con trazo simple por inscritos en el mismo arco y los de trazo triple por ser CM la bisectriz). Por ello:

$$\frac{a}{\overline{MC}} = \frac{\overline{DC}}{b} \Leftrightarrow a \cdot b = \overline{DC} \cdot \overline{MC} = \overline{DC} \cdot (\overline{DC} + \overline{MD}) =$$

$$= \overline{DC}^2 + \overline{DC} \cdot \overline{DM} = \overline{DC}^2 + \overline{DA} \cdot \overline{DB}$$

Copyrighted material

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

XVII

LOS MOVIMIENTOS EN EL PLANO

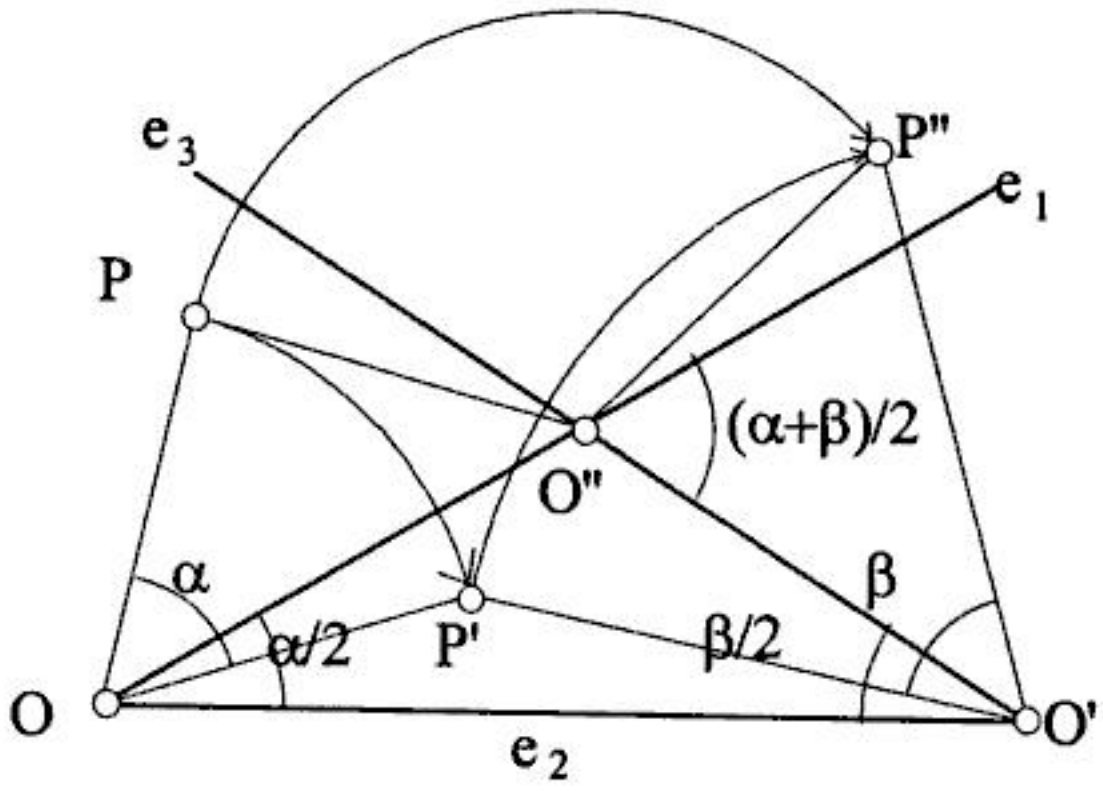
Copyrighted material

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

PRODUCTO DE DOS GIROS DE DIFERENTES CENTROS



Sea g el giro de centro O y amplitud α.

Sea f el giro de centro O' y amplitud β.

Queremos determinar la naturaleza de la transformación producto f·g.

En la figura se han visualizado aplicadas a un punto cualquiera P de modo que:

$f \cdot g(P) = f(g(P)) = f(P') = P''$

Vamos a descomponer cada giro en producto de dos simetrías de ejes concurrentes en el centro de giro.

Según se vio en el producto de simetrías de ejes no paralelos podemos descomponer un giro en producto de dos simetrías cuyos ejes concurren en el centro de giro y forman ángulo mitad de la amplitud del giro, pudiendo elegir la dirección de uno de los ejes.

El primer giro g se descompone en producto de las simetrías de ejes e_1 y e_2 siendo e_2 la recta OO' que une los centros y e_1 la que forma ángulo $\alpha/2$ con e_2.

El segundo giro f se descompone en producto de las simetrías de ejes e_2 y e_3 formando entre ellas ángulo $\beta/2$.

Designando a las simetrías por el mismo nombre que a sus ejes, para la transformación producto tenemos:

$$f \cdot g = e_3 \cdot e_2 \cdot e_2 \cdot e_1 = e_3 \cdot e_1$$

Lo que prueba que la transformación producto es un giro de centro O" (punto de corte de e_1 y e_3) y amplitud $\alpha + \beta$ según se establece fácilmente en la figura.

Una vez establecido el resultado, para construir el centro basta trazar las rectas e_2, e_1 y e_3.

La demostración anterior falla en el caso de que e_1 y e_3 sean paralelos.

Eso ocurrirá cuando $\alpha + \beta = 360°$ y en ese caso la transformación producto es una traslación de vector perpendicular a la dirección común de e_1 y e_3 y módulo el doble de la distancia entre ambos ejes como ya se demostró.

Copyrighted material

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

Si representamos por T a las traslaciones, por G a los giros, por S a las simetrías axiales y por R a las reflexiones-deslizamiento, el siguiente cuadro resume la estructura de los productos de todas las pareja posibles:

·	T	G	S
T	T	G	R
G	G	G/T	R
S	R	R	G/T

En la tabla se observa que las traslaciones y giros forman subgrupo.

Daremos un par de resultado clásicos que solucionan dos problemas de extremos mediante movimientos.

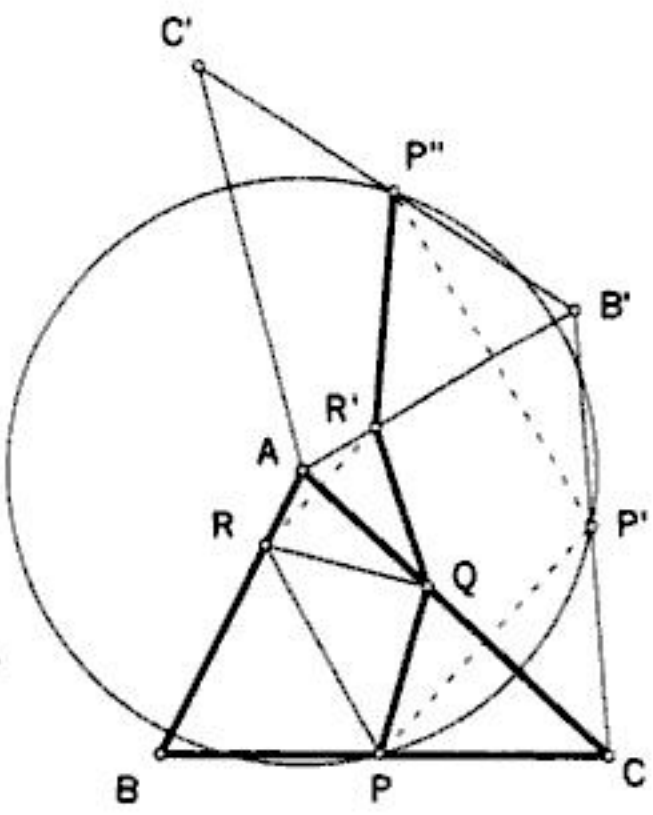
PROBLEMA DE FAGNANO

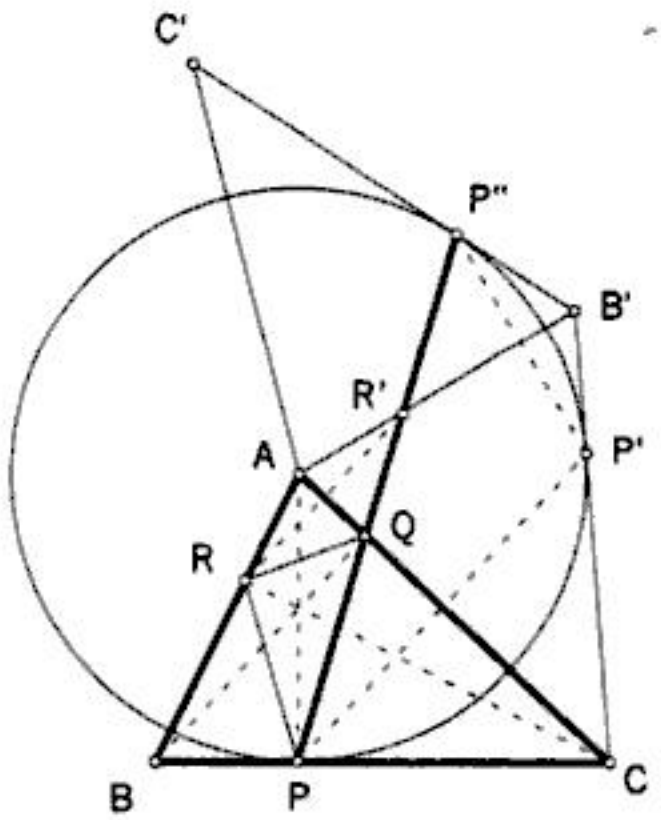
Dado un triángulo acutángulo ABC, inscribir un triángulo de perímetro mínimo.

Sea PQR el triángulo inscrito con P en BC, Q en AC y R en AB.

Haciendo dos simetrías sucesivas de ejes AC y AB', el triángulo dado se transforma en AB'C' y el perímetro de PQR en la poligonal PQR'P'' (figura de la izquierda).

Como la transformación producto es un giro de centro A y amplitud 2A, P'' está en la circunferencia de centro A y radio AP.





Copyrighted material

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

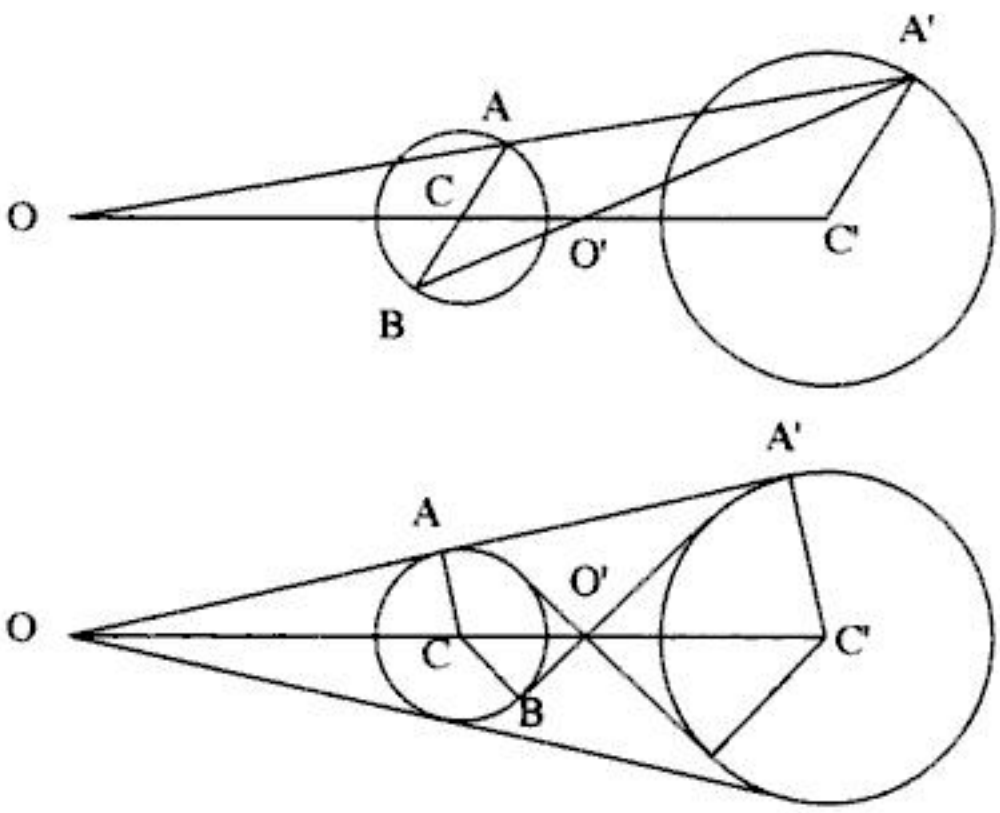
You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

1. CIRCUNFERENCIAS CONCÉNTRICAS

En este caso es obvio que la única homotecia con centro en el común de ambas circunferencias y razón $k = \frac{r'}{r}$ transforma la primera en la segunda.

2. CIRCUNFERENCIAS NO CONCÉNTRICAS



Demostraremos que en este caso hay dos homotecias que resuelven el problema.

En efecto, tomando un punto A cualquiera de la primera circunferencia (izquierda parte superior de la figura) y el punto diametralmente opuesto B, se trazan los radios correspondientes a A y B y en la segunda circunferencia el radio C'A' paralelo a CA.

Las intersecciones de la recta AA' con CC' y BA' con CC' nos dan los puntos O y O' centros de la homotecia buscadas.

Por la semejanza de ΔOAC y $\Delta OA'C'$, tenemos:

$$\frac{OA'}{OA} = \frac{OC'}{OC} = \frac{r'}{r}$$

Expresión que prueba que A y A' son homotéticos en una homotecia h de centro O y razón $\frac{r'}{r}$.

La misma expresión prueba que la posición de O no depende del punto A elegido y que los centros también se corresponden en la homotecia.

Análogas consideraciones reemplazando A por B nos dan la igualdad:

$$\frac{O'A'}{O'B} = \frac{O'C'}{O'C} = -\frac{r'}{r}$$

expresión que determina la segunda homotecia h' de centro O' y razón: $-\frac{r'}{r}$.

Como el punto A es cualquiera, para la construcción de los centros O y O' se suelen coger los puntos de tangencia de las tangentes comunes como se indica en la par-

Copyrighted material

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

Dado un punto O fijo del plano π y un número real k, definimos inversión de polo O y potencia k como la transformación geométrica del plano que a un punto P le hace corresponder otro P' tal que P' está alineado con O y con P y verificando:

$$\overline{OP} \cdot \overline{OP'} = k$$

Excluido O es una aplicación biyectiva.

Si k es positivo, P y P' están en la misma semirrecta respecto de O; si es negativo en distinta.

La inversión es una transformación involutiva. Es decir; si P' es el inverso de P, P lo es de P'. Escrito con notación funcional y llamando f a la inversión:

$$\forall P \in \pi: \qquad f(f(P)) = P$$

PUNTOS DOBLES

Si imponemos la condición P' = P, resulta que:

$$\overline{OP} \cdot \overline{OP} = k \Leftrightarrow \overline{OP} = \sqrt{k}$$

Por tanto, si $k<0$ no existen puntos dobles y si $k>0$ existen infinitos puntos dobles todos a la misma distancia $\sqrt{k}$ del polo. Forman la llamada circunferencia de autoinversión.

Obviamente una inversión de potencia $k<0$ es el producto de una inversión de potencia $|k|$ por una simetría central de centro el polo de inversión. Por ello, en lo que sigue supondremos que k es positivo.

Copyrighted material

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

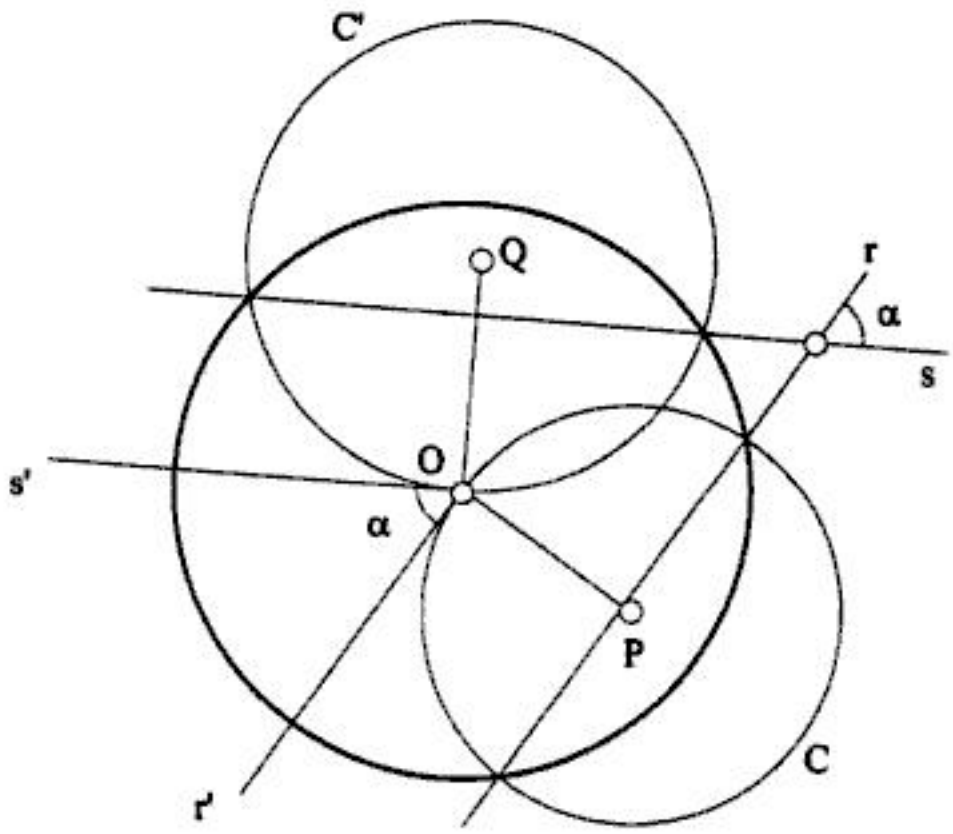
You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

iguales y la recta se llama isogonal respecto de las dos circunferencias C y C' al formar con ambas el mismo ángulo.

El recíproco también es cierto. Toda recta secante isogonal a dos circunferencias dadas pasa por el polo de inversión (o centro de homotecia) y por tanto es doble en ambas transformaciones.

CONSERVACIÓN DE ÁNGULOS EN LA INVERSIÓN

Sea una inversión de polo O, r y s dos rectas que no pasan por el polo y C, C' sus figuras inversas que, según lo demostrado antes, son dos circunferencias que pasan por O.



Si llamamos α al ángulo formado por r y s, vamos a demostrar que es el mismo que forman C y C'.

Según sabemos, el ángulo formado por dos circunferencias es el que determinan sus tangentes en el punto de intersección.

Como C y C' pasan por O, se han trazado las tangentes a ambas circunferencias designadas por r' y s' respectivamente.

El resultado es evidente ya que las tangentes r' y s' son paralelas a r y s por ser perpendiculares a los radios en los puntos de tangencia OP y OQ.

Por la propiedad involutiva de la inversión tambien queda probado para circunferencias que pasan por el polo. Para las que no pasan tambien es cierto, dado que la homotecia conserva los ángulos.

Finalmente si las rectas pasan por el polo, es trivial ya que son dobles.

En general toda transformación geométrica que conserva ángulos se denomina "conforme". Por ello decimos que la inversión es una transformación conforme.

Copyrighted material

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

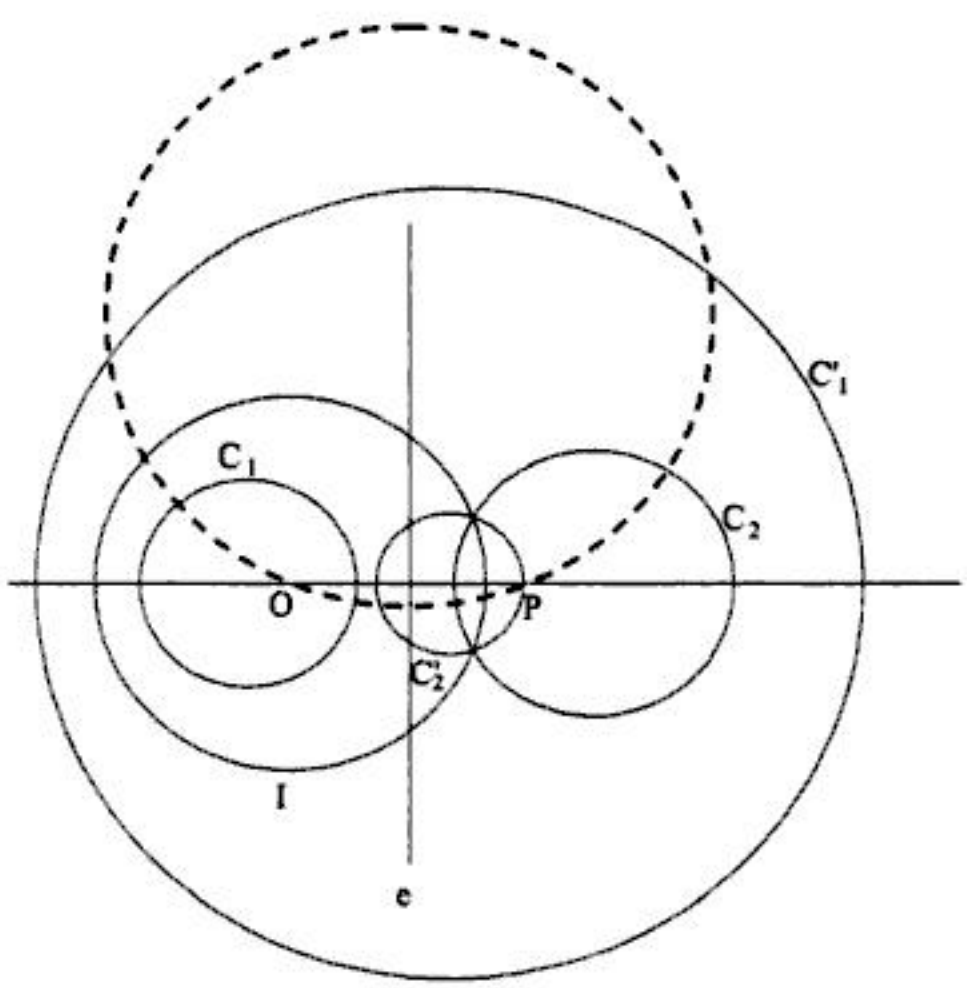
En efecto, las circunferencias dadas determinan un haz que es la imagen mediante inversión (o tiene por imagen mediante la misma inversión) de:

- Un conjunto de rectas concurrentes cuando el haz que determinan es elíptico.
- Un conjunto de circunferencias concéntricas cuando el haz es hiperbólico.
- Un conjunto de rectas paralelas cuando el haz es parabólico.

Es claro entonces que sólo es posible transformar las circunferencias dadas en otras concéntricas cuando determinan un haz hiperbólico o, lo que es equivalente, cuando no tienen ningún punto común.

En ese caso existen dos polos de inversión y para cada uno de ellos infinitos valores de la potencia. Los polos son los puntos que en la figura de la página anterior se designaron por O y P. Esos puntos se denominan vértices o puntos límite del haz hiperbólico correspondiente.

En la figura siguiente se da la construcción de tales puntos y de una inversión que transforma dos circunferencias dadas en otras dos concéntricas.



En la figura se supone que las dos circunferencias de partida son exteriores pero la construcción es muy parecida si una es interior a la otra. La única diferencia está en la construcción del eje radical que está explicada en el tema correspondiente para el caso de circunferencias interiores.

Suponiendo que las circunferencias dadas son C_1 y C_2, los pasos para la construcción son los siguientes:

1. Se traza la línea que une los centros.
2. Se construye el eje radical e.
3. Se traza una circunferencia con centro en el eje radical que sea ortogonal a C_1 y C_2 (de trazos en la figura).
4. Los puntos de intersección de la circunferencia del paso 3 con la recta del paso 1 (O y P) son los puntos límites del haz. Cualquiera de ellos vale como polo de inversión.

Copyrighted material

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

XX LUGARES GEOMÉTRICOS

Copyrighted material

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

MÉTODO DE TRANSFORMACIONES GEOMÉTRICAS

Básicamente consiste en identificar el lugar pedido como la imagen de algún lugar conocido mediante una transformación geométrica también conocida.

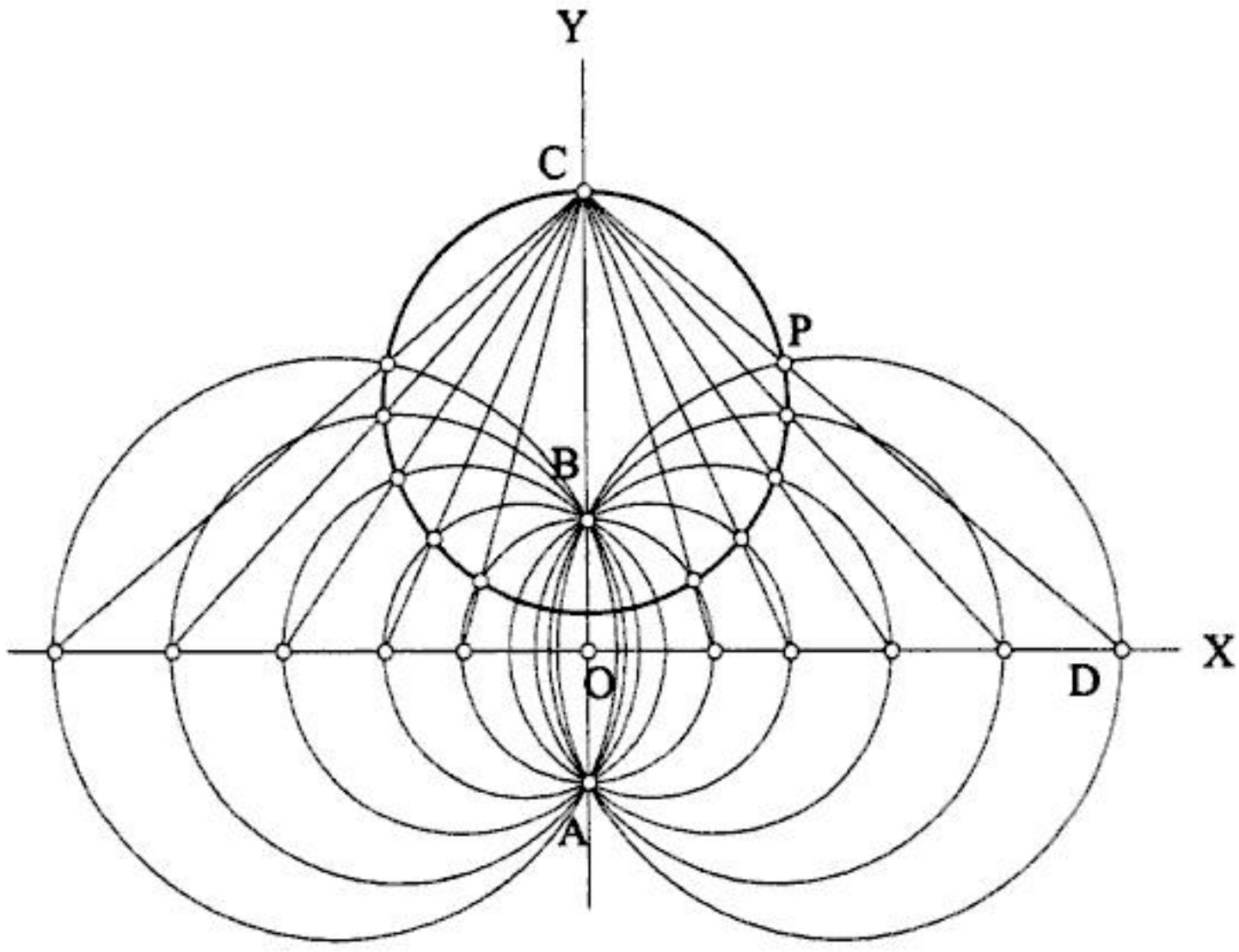
Las transformaciones más usuales son traslaciones, giros, simetrías, homotecias e inversiones.

Para establecer el método se intenta ligar los puntos pedidos con otros que pertenezcan a un lugar geométrico conocido mediante alguna relación que exprese una transformación de las anteriores o una sucesión (producto) de ellas.

Por supuesto que muchos problemas de lugares geométricos salen por más de un método, pero siempre es interesante intentar éste por lo rápido y elegante.

Suele ser definitivo hacer un buen dibujo y señalar varios puntos.

EJEMPLO 3



Dados tres puntos alineados A, B, C se toma un punto variable D sobre la mediatriz de AB. Se traza la circunferencia que pasa por A, B y D. Se traza la recta CD que corta a la circunferencia en segundo punto P. Hallar el lugar de P al variar D en la mediatriz.

Copyrighted material

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

10. El lugar geométrico de los puntos cuya razón de distancias a dos puntos dados A, B es constante es una circunferencia cuyo centro está alineado con A y B.
11. El lugar geométrico de los puntos desde los cuales se ven dos circunferencias dadas bajo ángulos iguales, es otra circunferencia cuyo centro está alineado con los de las circunferencias dadas.
12. El lugar geométrico de los puntos cuya suma de cuadrados de distancias a dos puntos dados A, B es constante es una circunferencia cuyo centro está alineado con A y B.

Copyrighted material

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

58. Calcular $\sum_{k=5}^{k=49} \frac{11_{(k}}{\sqrt[3]{1331_{(k}}}$ sabiendo que 11 y 1331 están escritos en base $k > 3$.

59. Demostrar que en el triángulo ABC, de lados $a \geq b \geq c$:

$$\frac{aA + bB + cC}{a + b + c} \geq \frac{\pi}{3}$$

60. Calcular: $\lim_{n \to \infty} \frac{1}{n} \sqrt[n]{(n+1)(n+2)....(2n)}$

61. De entre los números 1, 2, 3, ..., 2n, se eligen de cualquier forma (n + 1) distintos. Demostrar que entre los números elegidos hay por lo menos dos tales que uno es divisor del otro.

62. Demostrar: $\forall n \in N \text{ y } n > 1 \Rightarrow n! < \left(\frac{n+1}{n}\right)^n$

63. En un grupo de 24 alumnos de COU que han escogido al menos una de las asignaturas de Filosofía, Geografía y Matemáticas, 5 alumnos escogen Filosofía y Geografía, 3 Filosofía y Matemáticas, 6 Geografía y Matemáticas. El número de los que escogen sólo una de esas asignaturas es el mismo para las tres. ¿Qué número de alumnos ha escogido cada una de esas asignaturas?

64. Sea un prisma hexagonal regular. ¿Cuál es la poligonal que partiendo de un vértice de la base, recorre todas las caras laterales y termina en el vértice de la cara superior, situado en la misma arista que el vértice de partida, y tiene longitud mínima?

65. Se consideran en el plano los conjuntos de números complejos:

$$A = \left\{ z \mid \arg[z - (2 + 3i)] = \frac{\pi}{4} \right\} \qquad B = \left\{ z \mid |z - (2 + i)| < 2 \right\}$$

Determinar la proyección ortogonal del conjunto intersección de A y B sobre el eje OX.

66. Dadas dos rectas r, r' y un punto P que pertenece al plano que determinan las rectas pero no pertenece a ninguna de ellas, determinar un triángulo equilátero que tenga por vértice el punto P y los otros dos vértices cada uno sobre una recta.

67. Demostrar que $A_n = 5^n + 2.3^{n-1} + 1$, es múltiplo de 8 para todo entero positivo n.

68. Expresar el inverso de 3 en el cuerpo Z/(p), siendo p primo, en función de p.

69. Hallar la inversión que transforma tres puntos no alineados A,B,C en los vértices de un triángulo equilátero.

Copyrighted material

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

137. Un número entero se escribe con tres cifras distintas. Obtenemos tres números de dos cifras cada uno suprimiendo la cifra de las centenas, la de las decenas y la de las unidades. La suma de estos tres números es la mitad del número de tres cifras inicial. Hallarlo.

138. En la isla de Camelot viven 13 camaleones rojos, 15 verdes y 17 amarillos. Cuando dos de distinto color se encuentran, cambian simultáneamente al tercer color. ¿Podría darse la situación en la que todos tengan el mismo color?

139. Sobre una cinta métrica de dos metros subdividida en milímetros, señalamos un trazo verde cada 11 mm y un trazo rojo cada 17 mm, ambos comenzando desde el mismo extremo. Hallar cuántos trazos verdes están a 1mm de un trazo rojo.

140. Un gato está quieto a la izquierda de una ratonera (considerada como un punto) acechando la salida de algún ratón. Sale un ratón que huye hacia la derecha lo más rápido que puede. El gato corre tras él y lo atrapa. Cuando se dispone a devorarlo ve cómo sale un segundo ratón que huye hacia la izquierda a la misma velocidad que el primero. El gato sale en su persecución y atrapa a su segunda víctima después de una carrera que dura cinco veces más que la anterior. De nuevo se dispone a comérselo cuando ve salir un tercer ratón que huye hacia la derecha algo más despacio que los anteriores debido al reuma que padece. El gato sale tras él y lo caza en un tiempo doble del empleado para el segundo ratón. Con estos datos se trata de hallar la relación Vs/Vr siendo Vs la velocidad del ratón sano y Vr la del ratón con reuma.

141. Los profesores y alumnos de un instituto son entre todos 1991 personas. En una excursión han de atravesar un río para lo que disponen de una sola barca. La barca no puede llevar a la vez más de 100 kilos. Cada alumno pesa 50 kilos y cada profesor 100 (la sabiduría es muy pesada). Se necesitan como mínimo 4235 travesías para que pasen todos. Hallar el número de profesores y el de alumnos. (Cada viaje de ida y vuelta son dos travesías).

142. ABC es un triángulo isósceles, r y R los radios de los círculos inscrito y circunscrito respectivamente y d la distancia entre el incentro y el circuncentro. Demostrar que:

$$d^2 = R^2 - 2Rr.$$

143. Encontrar todos los números naturales n tales que $2^n - 1$ es divisible por 7. Demostrar que no hay ningún natural p tal que $2^p + 1$ es divisible por 7.

144. Dada la sucesión de Fibonacci:

$$a_1 = a_2 = 1 \qquad \forall n \geq 2 \quad a_{n+1} = a_n + a_{n-1}.$$

Copyrighted material

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

199. La ecuación $x^3+ ax^2+ bx+ c = 0$ (c no nulo) tiene tres raíces distintas en progresión geométrica y cuyos inversos pueden ordenarse de modo que formen progresión aritmética. Hallar b y c en función de a.

200. Sea ABC un triángulo cualquiera. Exteriormente a él se construyen dos cuadrados BAEP y ACRD de lados AB y AC, respectivamente. Sean M y N, respectivamente, los puntos medios de BC y ED. Demostrar que AM es perpendicular a ED y que AN es perpendicular a BC.

Copyrighted material

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

UNIVERSITAS

En cada grupo de alumnos hay un porcentaje de ellos que **tienen lo que se puede llamar "gusto por las matemáticas", que no se preguntan ¿para qué sirve esto? El reto de intentar resolver un problema y la satisfacción de conseguirlo es suficiente motivación.**

Este MANUAL DE MATEMÁTICAS PARA PREPARACIÓN OLÍMPICA, intentando paliar tremendas lagunas, recoge cuestiones básicas como la divisibilidad, y nociones elementales de teoría de números, ecuaciones diofánticas, congruencias y geometría métrica, ausentes por completo de los programas de matemáticas de la enseñanza media, y de gran incidencia en las Olimpiadas Matemáticas.

Una aportación muy esperada -especialmente valiosa por la originalidad de los problemas propuestos y la presentación teórica de cada capítulo, que incluye problemas resueltos de fácil comprensión- que será de gran utilidad tanto para alumnos y profesores de cara a la preparación para diferentes pruebas y concursos de matemáticas, como para todas aquellas personas aficionadas a la resolución de problemas.

UNIVERSITAT JAUME·I

Cristóbal Sánchez-Rubio y Manuel Ripollés son catedráticos de Matemáticas de enseñanza media con más de 25 años de experiencia en institutos de Castellón.
En los últimos años han trabajado en la preparación y organización de Olimpiadas de Matemáticas de ámbito provincial y estatal.

ISBN 978-84-8021-319-6

Copyrighted material